



HOMELAND SECURITY

An Introduction to Principles and Practice

Fourth Edition

Charles P. Nemeth



CRC Press
Taylor & Francis Group

Homeland Security



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Homeland Security

An Introduction to Principles and Practice

Fourth Edition

Charles P. Nemeth



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Fourth edition published 2021
by CRC Press
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

and by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

© 2021 Charles P. Nemeth

First edition published by CRC Press 2009

Sixth edition published by Routledge 2016

CRC Press is an imprint of Informa UK Limited

The right of Charles P. Nemeth to be identified as author of this work has been asserted by him in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this book may be reprinted or reproduced or utilised in any form or by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying and recording, or in any information storage or retrieval system, without permission in writing from the publishers.

For permission to photocopy or use material electronically from this work, access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. For works that are not available on CCC please contact mpkbookspermissions@tandf.co.uk

Trademark notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data

Names: Nemeth, Charles P., 1951- author.

Title: Homeland security : an introduction to principles and practice /

Charles P. Nemeth.

Description: 4 Edition. | Boca Raton : CRC Press, 2021. | Revised edition of the author's Homeland security, [2017] | Includes bibliographical references and index. | Summary: "Homeland Security: An Introduction to Principles and Practice, Fourth Edition continues its record of providing a fully updated, no-nonsense textbook to reflect the latest policy, operational, and program changes to the Department of Homeland Security (DHS) over the last several years. The blend of theory with practical application instructs students on how to understand the need to reconcile policy and operational philosophy with the practical application of technologies and implementation of practices. The homeland security landscape of today is vastly different of that immediately following 9/11 and back when DHS was established in November of 2002. Domestic and international terrorism, gun violence, the geopolitical landscape, critical infrastructure security challenges, pandemic response-particularly with COVID-19-and disaster management have all become more complex and increasingly imperative. The new edition is completely updated to reflect changes to both new challenges and continually changing considerations. This includes: facial recognition, intelligence gathering techniques, information sharing databases, white supremacy, domestic terrorism and lone wolf actors, border security and immigration, the use of drones and surveillance technology, cybersecurity, the status of ISIS and Al Qaeda, the increased nuclear threat, COVID-19, ICE, DACA, and immigration policy challenges-among numerous others. Consideration of, and the coordinated response, to all these is housed among a myriad of federal agencies and departments. Homeland Security, Fourth Edition continues to serve as the comprehensive and authoritative text. The book presents the various DHS state and federal agencies and entities within the government-their role, how they operate, their structure, and how they interact with other agencies-to protect U.S. domestic interests from various dynamic threats"— Provided by publisher.

Identifiers: LCCN 2021001614 (print) | LCCN 2021001615 (ebook) |

ISBN 9780367494414 (hardback) | ISBN 9781003176053 (ebook)

Subjects: LCSH: United States. Department of Homeland Security. | National security—United States. | Terrorism—United States—Prevention.

Classification: LCC HV6432.4 .N46 2021 (print) | LCC HV6432.4 (ebook) |

DDC 353.30973—dc23

LC record available at <https://lcn.loc.gov/2021001614>

LC ebook record available at <https://lcn.loc.gov/2021001615>

ISBN: 978-0-367-49441-4 (hbk)

ISBN: 978-1-032-01651-1 (pbk)

ISBN: 978-1-003-17605-3 (ebk)

Typeset in Minion Pro
by codeMantra

Access the Support Material: www.routledge.com/9780367494414

To Stephen Charles Nemeth, a former Marine officer, gentleman, and the type of son and man that impresses each and every day.

To St. Thomas Aquinas who remarked:

Nothing hinders one act from having two effects, only one of which is intended, while the other is beside the intention. Now moral acts take their species according to what is intended, and not according to what is beside the intention, since this is accidental as explained above.

Accordingly the act of self-defense may have two effects, one is the saving of one's life, the other is the slaying of the aggressor. Therefore this act, since one's intention is to save one's own life, is not unlawful, seeing that it is natural to everything to keep itself in "being," as far as possible.

Summa Theologica II-II, Question 64, Article 7



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Contents

Preface.....	xv
Acknowledgments.....	xix
Author.....	xxi
Introduction.....	xxiii
 Chapter 1 The Idea and Origin of Homeland Security.....	1
1.1 Introduction.....	1
1.2 Threats to the Homeland: Twentieth-Century Military Movements	2
1.3 Threats to the Homeland: The Cold War Experience.....	6
1.4 Threats to the Homeland: Iran, Terror, and the World Stage.....	14
1.5 Threats to the Homeland: North Korea: An Old and New Enemy in the War on Terror	19
1.6 Threats to the Homeland: Revolution, Riot, and Rightful Demonstration	22
1.6.1 Domestic Terrorism: Pre-9/11.....	23
1.6.2 International Terrorism: Pre-9/11	29
1.7 Conclusion	30
Keywords.....	31
Discussion Questions	31
Practical Exercises.....	32
Notes.....	32
 Chapter 2 Terror, Threat, and Disaster Post 9/11: A New Paradigm of Homeland Security.....	35
2.1 Introduction.....	36
2.2 Genesis of DHS.....	38
2.3 DHS: 2001–2003	46
2.3.1 Evolution and Change in DHS.....	46
2.4 Reorganization and Evolution of DHS: 2003–2015.....	49
2.5 DHS in the Age of President Donald J. Trump: 2016–2021	51
2.5.1 Office of the Secretary of DHS.....	51
2.5.2 DHS Directorates.....	63
2.5.2.1 Cybersecurity and Infrastructure Security Agency (CISA): Former Directorate for National Protection and Programs.....	63
2.5.2.2 Directorate for Science and Technology	66

Contents

- 2.5.2.3 Directorate for Management 68
 - 2.5.3 DHS Offices: Support and Operational Components..... 69
 - 2.5.4 Agencies and Entities Swept into DHS 73
 - 2.5.4.1 U.S. Coast Guard.....73
 - 2.5.4.2 U.S. Secret Service..... 79
 - 2.5.4.3 Federal Law Enforcement Training Center 83
 - 2.5.5 Advisory Panels and Committees 86
 - 2.6 Conclusion 87
 - Keywords..... 88
 - Discussion Questions 88
 - Practical Exercises..... 89
 - Notes..... 89
- Chapter 3 Homeland Security Law, Regulations, and Budgeting.....93
 - 3.1 Introduction.....93
 - 3.2 Homeland Security Law, Regulations, and Executive Orders..... 94
 - 3.2.1 Executive Order 13228: Origin of DHS 94
 - 3.2.2 Executive Order 13231: Protection of Infrastructure 94
 - 3.2.3 Executive Order 13223: September 14, 2001 94
 - 3.2.4 Executive Order 13493 of January 22, 2009..... 98
 - 3.2.5 Executive Order 13567 of March 7, 2011 103
 - 3.2.6 Executive Order 13846 of August 6, 2018 104
 - 3.2.7 Homeland Security Act of 2002..... 104
 - 3.2.7.1 Homeland Security Act and Posse Comitatus 106
 - 3.2.8 USA Patriot Act: USA Freedom Act of 2015.....107
 - 3.2.9 Specialized Laws 109
 - 3.2.9.1 REAL ID Program 109
 - 3.2.9.2 Office of Biometric Identity Management
(Formerly Office of US-VISIT).....112
 - 3.2.9.3 Chemical Facilities.....113
 - 3.2.9.4 Invention and Technology: The SAFETY Act.....114
 - 3.3 Budgeting, Finance, and Funding in Homeland Security 115
 - 3.3.1 Budget Year: 2003 115
 - 3.3.2 Budget Year: 2004.....118
 - 3.3.3 Budget Year: 2005 123
 - 3.3.4 Budget Year: 2006 130
 - 3.3.5 Budget Year: 2007 134
 - 3.3.6 Budget Year: 2008 138
 - 3.3.7 Budget Years: 2009–2010 142
 - 3.3.8 Budget Years: 2011–2012 142
 - 3.3.9 Budget Year: 2013.....147
 - 3.3.10 Budget Year: 2014.....149
 - 3.3.11 Budget Year: 2015.....152
 - 3.3.12 Budget Year: 2016.....153
 - 3.3.13 Budget Year: 2017.....156
 - 3.3.14 Budget Year: 2018.....157
 - 3.3.15 Budget Year: 2019.....160
 - 3.3.16 Budget Year: 2020 162

3.4	Conclusion	163
	Keywords.....	164
	Discussion Questions	165
	Practical Exercises.....	165
	Notes.....	165
Chapter 4	Risk Management, Threats, and Hazards	171
4.1	Introduction.....	171
4.2	Risk Management	172
4.2.1	The Nature of Risk.....	172
4.2.2	Risk Assessment.....	174
4.2.3	CARVER+Shock Assessment Tool.....	180
4.3	Threats and Hazards.....	185
4.3.1	Concept of Threat and Hazard	186
4.3.2	Weapons of Mass Destruction	190
4.3.2.1	Nuclear.....	190
4.3.2.2	Radiological	196
4.3.2.3	Biological	198
4.3.2.4	Chemical.....	206
4.3.2.5	Improvised Explosive Devices.....	218
4.4	Computer Security and Information Infrastructure.....	222
4.4.1	Cyber Challenges and the American Electoral Process.....	227
4.4.2	National Cyber Security Division	228
4.4.3	US-CERT: Computer Emergency Response Team	229
4.5	Private Sector and Homeland Security.....	232
4.6	Conclusion	239
	Keywords.....	240
	Discussion Questions	241
	Practical Exercises.....	241
	Notes.....	242
Chapter 5	Training and Exercises in Homeland Security.....	249
5.1	Introduction.....	249
5.2	Grants and Training.....	251
5.3	Center for Domestic Preparedness.....	260
5.4	Emergency Management Institute	261
5.5	Homeland Security Exercise and Evaluation Program	265
5.6	Lessons Learned: Best Practices (LLIS.GOV)/Homeland Security Digital Library (HSDL).....	270
5.7	Community Emergency Response Teams.....	272
5.8	National Incident Management System.....	274
5.9	Conclusion	281
	Keywords.....	282
	Discussion Questions	285
	Practical Exercises.....	285
	Notes.....	285

Contents

Chapter 6 DHS Challenges: National versus State and Local, National Security versus Homeland Security..... 289

6.1 Introduction..... 289

6.2 Challenge of National Policy at the State and Local Levels 290

6.2.1 Structure at the State Level..... 292

6.2.2 Structure at the Local Level..... 296

6.2.2.1 Fusion Centers..... 298

6.2.3 Funding and Local Initiatives.....319

6.3 Fine Line of National Defense and Homeland Security..... 322

6.3.1 Department of Defense and Homeland Security..... 327

6.3.2 Intelligence Gathering and Sharing.....331

6.3.2.1 Office of Naval Intelligence.....331

6.3.2.2 Air Force Intelligence 334

6.3.2.3 U.S. Marine Corps 335

6.3.2.4 U.S. Army.....337

6.3.2.5 United States Coast Guard Intelligence 339

6.3.3 Specialized Military/Defense Units Dedicated to Homeland Security..... 340

6.3.3.1 National Maritime Intelligence-Integration Office (NMIO) 340

6.3.3.2 National Reconnaissance Office..... 340

6.3.3.3 Weapons of Mass Destruction Civil Support Teams 341

6.4 Conclusion 346

Keywords..... 347

Discussion Questions 347

Practical Exercises..... 348

Notes..... 348

Chapter 7 FEMA, Response, and Recovery 351

7.1 Historical Foundation for FEMA 351

7.1.1 Federal Emergency Management Agency: Pre-9/11 352

7.1.2 Federal Emergency Management Agency: Post-9/11.....352

7.2 FEMA and Preparedness.....357

7.2.1 Role of Mitigation in the Preparedness Model..... 367

7.3 FEMA Response and Recovery.....378

7.3.1 National Response Framework..... 380

7.4 Conclusion 383

Keywords..... 384

Discussion Questions 385

Practical Exercises..... 385

Notes..... 385

Chapter 8 Intelligence 389

8.1 Introduction..... 389

8.2 Intelligence..... 390

8.3 Terror, Threats, Disaster, and Intelligence Agencies..... 395

8.3.1	Federal Bureau of Investigation.....	396
8.3.1.1	Joint Terrorism Task Forces.....	401
8.3.1.2	National Security Branch.....	403
8.3.1.3	NSB and the WMD Directorate.....	404
8.3.2	Central Intelligence Agency.....	409
8.3.2.1	Directorate of Analysis.....	410
8.3.2.2	Directorate of Operations: Clandestine Services..	412
8.3.2.3	Directorate of Science and Technology.....	412
8.3.2.4	Directorate of Digital Innovation	412
8.3.2.5	Directorate of Support.....	413
8.3.2.6	Mission Centers.....	413
8.3.3	Offices of the Director of National Intelligence	414
8.3.3.1	National Counterterrorism Center.....	417
8.3.3.2	National Counterintelligence and Security Center.....	418
8.3.3.3	National Intelligence Council	420
8.3.4	Defense Intelligence Agency	423
8.4	Conclusion	424
	Keywords.....	425
	Discussion Questions	426
	Practical Exercises.....	426
	Notes.....	427
Chapter 9	Border Security, U.S. Citizenship, and Immigration Services	429
9.1	Introduction.....	429
9.2	U.S. Customs and Border Protection	430
9.2.1	Border Protection	434
9.2.1.1	Secure Border Initiative: Its Creation and Demise	438
9.2.1.2	CBP Air and Marine	446
9.2.2	CBP and the Facilitation of Trade and Commerce.....	449
9.2.2.1	Cargo.....	451
9.3	U.S. Citizenship and Immigration Services.....	460
9.3.1	Current Challenges in Immigration	464
9.3.1.1	Sanctuary Jurisdictions	464
9.3.1.2	The DACA Dilemma.....	464
9.3.1.3	The Visa Lottery Program	467
9.3.1.4	The Complexity of Chain Migration	467
9.3.2	Project Shield America Initiative.....	469
9.3.3	Fugitive Operations Program	470
9.3.4	Cornerstone Initiative	471
9.3.5	Cyber Crimes Center.....	472
9.3.6	US-VISIT Program/Office of Biometric Identity Management.....	475
9.4	Conclusion	476
	Keywords.....	477
	Discussion Questions	477
	Practical Exercises.....	477
	Notes.....	477

Contents

Chapter 10	Transportation Security.....	481
10.1	Introduction.....	481
10.2	Transportation Security Administration	482
10.2.1	TSA and the Privatized Airport	488
10.2.2	Federal Air Marshals.....	490
10.2.3	Federal Flight Deck Officers.....	491
10.2.4	Law Enforcement Officers Flying Armed	493
10.2.5	TSA's Canine Explosive Detection Unit	493
10.2.6	Risk Management Programs.....	493
10.2.7	TSA Technology and Innovation	497
10.2.7.1	Trace Portals and Their Demise.....	497
10.2.7.2	Millimeter Wave/Advanced Imaging Technology.....	498
10.2.7.3	Biometrics	501
10.3	Maritime Security.....	508
10.3.1	National Strategy for Maritime Security.....	510
10.3.2	Other Maritime Plans	511
10.3.2.1	National Plan to Achieve Maritime Domain Awareness.....	512
10.3.2.2	Maritime Transportation System Security Plan...512	
10.3.3	DHS: Borders and Marine Division	512
10.3.4	Role of the Coast Guard in Maritime Security.....	513
10.3.4.1	Emergency Safety	515
10.3.4.2	Security and Law Enforcement	517
10.3.4.3	Cargo and Ports.....	522
10.4	Rail and Mass Transit.....	534
10.4.1	Representative Security Programs for Rail and Transit....	541
10.4.1.1	Amtrak.....	542
10.4.1.2	CSX: The Freight Line.....	544
10.4.1.3	SEPTA: Rail Mass Transit.....	546
10.5	Conclusion	549
	Keywords.....	555
	Discussion Questions	555
	Practical Exercises.....	556
	Notes.....	556
Chapter 11	Homeland Security and Public Health.....	561
11.1	Introduction: Public Health and Homeland Security	561
11.2	Water and Public Health.....	565
11.3	Agriculture, Food, and Public Health	569
11.3.1	Strategic Partnership Program on Agroterrorism.....	575
11.3.2	Infectious Animals	578
11.3.3	Infectious Diseases, Bioterrorism, and Public Health.....	581
11.3.3.1	Project BioShield	587
11.3.3.2	Strategic National Stockpile.....	588
11.3.3.3	National Select Agent Registry Program	588
11.4	Pandemic Threats and Public Health.....	590
11.4.1	COVID-19: The Pandemic from China.....	595

11.4.2 Planning, Preparedness, and Response to the Pandemic	602
11.4.3 Response and Recovery under COVID-19.....	610
11.5 Conclusion	610
Keywords.....	616
Discussion Questions	616
Practical Exercises.....	616
Notes.....	617
 Chapter 12 The Future of Homeland Security.....	 621
12.1 Introduction.....	621
12.2 Growth without Reason.....	625
12.3 Curbing Expansionism in Mission.....	627
12.4 The Merits of Decentralization	629
12.5 The Rise of Technology	631
12.6 The Need for a New Way of Thinking: Jump Out of the Box	636
Notes.....	637
 Appendix A: United States Department of Homeland Security: Homeland Security Advisory Council.....	 639
 Appendix B: NIMS Implementation Objectives for Federal Departments and Agencies.....	 643
 Appendix C: Sanctuary Cities List	 647
 Appendix D: Incident Notification and Reporting Form	 655
 Appendix E: FEMA Strategic Plan Performance Measures.....	 661
 Index	 669



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Preface

This is a book about the very complex and highly bureaucratic world of Homeland Security. It is a humble attempt to give order to a mighty colossus of agencies and personnel dedicated to the protection of the homeland. At the commencement of this project, I never envisioned the “bigness” of the undertaking—the interweaving and entangling roles of people and departments and the sweep of the endeavor. Homeland Security, by any measure, is a massive enterprise that gets larger by the moment. Much of the growth arises from our understanding of things—what was once mostly a TSA/aircraft threat evolved into a multidimensional operation. While surely aircraft and passengers remain, the book makes plain that just about everything in life has a homeland quality to it. Whether it is food or water, military or private sector justice, or the border on land or sea, the task of protecting the homeland is a work in progress. Homeland Security extends its influence to all sectors of the economy, the business and corporate world, law enforcement and military branches, as well as communities, towns, and cities. What is just as striking is how regularly new homeland security concerns emerge and evolve. For example, the virtual world of cyberspace is now a pressing concern once undreamt of as is the rise of the “lone wolf” operating with similar passion and irrationality but without the organized planning. And in the FEMA world, the array of natural and man-made disasters seems to be ramping up over the last few years, especially as relates to flooding. The point is homeland security has never been a static concern.

Chapter 1 provides a foundational look at how our present system emerged by looking at the history of security threats in the American experience. In particular, the chapter considers how the Cold War period shaped our present policy on the homeland front and, just as importantly, how domestic forms of terrorism edify the DHS mindset and mentality. The protesters of the 1970s tell us much about the motive and method of terrorists as does the KKK Klansman, the spy engaged in espionage, and the anti-government zealot seeking to topple the established order. This pre-9/11 perspective is critical to any contemporary understanding of the homeland system.

Chapter 2 sees the world in the prism of events leading up to 9/11 and the subsequent evolution of policy and practice after these cataclysmic events. It is clear that a security outlook existed before 9/11, although that vision would be forever altered after the attack on the Twin Towers. Soon after these horrid events, the reaction of government and policymakers was to erect an agency and systematic response to these types of tragedies. The most obvious change in operational protocols relates to the “sharing” of information and the collaboration between agencies. The chapter zeroes in on the original version of the Department of Homeland Security (DHS) and its subsequent evolution and change. The DHS of 2002 was subject to many forces as leaders continuously sought more effective means of domestic protection. From 2003 and onward, diverse governmental entities were swept into the environs of DHS, from the Coast Guard to the Secret Service. Exactly how those adjustments and alterations came about and how these actions impacted the safety of our nation is closely scrutinized.

Chapter 3 stresses the legal basis and foundation for DHS. Exactly what laws, executive orders, and rulemaking made DHS possible? What is the primary legislation that enabled DHS? What other acts or laws govern homeland practice? Specific coverage includes the Patriot Act and the Homeland Security Act as well as specialized promulgations that deal with identity, chemical

Preface

facilities, and safety practice. At the same time, the debate over privacy issues continues to escalate especially because of the FISA court abuses exposed during the 2016–2020 political season. It is quite disheartening to see how intelligence and law enforcement agencies can be used to undermine political opponents. The chapter also highlights the budgetary commitment of lawmakers entrusted with the defense of a nation. From 2001 to 2009, budgets reflect the urgency of policymakers and the central mission of DHS. The genealogy of the budget is keenly reviewed since the DHS's emphasis will shift and move dependent on new threats or a better understanding of earlier homeland principles. With a longer-term perspective, we also witness how agency funding is impacted by not only new and novel challenges but also a winnowing out of inefficient processes in homeland security.

The nature of risk and threat is fully examined in Chapter 4. What is risk? What is a threat? How is risk defined and calculated? What types of risk and threat exist—merely nuclear, biological, and chemical? Other coverage includes risk measuring systems such as CARVER. The chapter expends considerable energy evaluating and distinguishing the world of threats and risk. Threats take many forms, including man-made and natural varieties. Special attention is given to biological and chemical threats, including plague, ricin, nerve agents, and dirty bombs. Finally, the chapter highlights how computer breaches are a new form of security risk in the world of Homeland Security and how US-CERT and the National Cyber Security Division and a host of new entities and programs address these issues. Of course, this chapter like all others expends some time on the challenges associated with the COVID-19 pandemic.

Chapter 5 introduces the reader to the world of training and preparatory exercises for the homeland professional. Within DHS resides a major infrastructure of offices dedicated to the funding and actual training for Homeland Security eventualities. Offices such as the Grants and Training, the Homeland Security Exercise and Evaluation Program (HSEEP), the Emergency Management Institute (EMI), and the Center for Domestic Preparedness are fully examined. Past security practices are evaluated within the DHS Lessons Learned program, which stores experiences and results from homeland protection policy and practice. It also highlights how the COVID-19 pandemic has impacted training. The chapter ends with a comprehensive look at NIMS—the National Incident Management System—which provides guidance and an operational methodology for hospitals, educational institutions, and other entities seeking to prevent threats.

Chapter 6 assesses the operational demands evident in the world of Homeland Security. More specifically, the chapter gauges how states and localities, which are considered the frontline of Homeland Security, can work compatibly with federal policymakers. A highly successful example of this cooperative mentality can be discovered in the funding mechanism for homeland grants and training allotments as well as the regional Fusion Centers that feed state and local information to the larger federal system. In addition, the chapter evaluates the fine line between civilian homeland function and that historically and contemporaneously assumed by the nation's military infrastructure. How do the various offices of intelligence in the military model share with DHS? Are the agencies and functions properly aligned? The chapter ends with a look at specialized entities and agencies that support the role and work of states and localities as these governmental authorities seek to advance the mission of DHS.

Chapter 7 targets the Federal Emergency Management Agency (FEMA) in both the pre- and post-9/11 world. Of all the agencies undergoing a transformation in mission and purpose since 9/11, none has been as dramatic as FEMA. FEMA has transformed itself from an agency dedicated to natural disaster to one concerned about the functions and tactics of response and recovery. Even FEMA gives advice and policy suggestions regarding the pandemic. The chapter examines the National Response Framework that provides protocol steps in the event of natural or man-made disasters and poses many examples of the agency's educational and mitigation function that prevents the full effect of disasters.

Chapter 8 delves into the world of intelligence. Aside from its definition and methodology, the stress is on the agencies and entities entrusted with intelligence analysis. Special attention is given to the FBI and its Joint Terrorism Task Forces and the CIA, whose various Directorates

aid DHS in its overall mission. The CIA's Directorates on Intelligence, Clandestine Activities, Science and Technology, and Support make major contributions to intelligence practice in the world of Homeland Security. On top of this, the chapter provides a summary review of the Defense Intelligence Agency and its intelligence functions and the role of the Office of the Director of National Intelligence that seeks to be a central repository for intelligence gathering across all government agencies.

The subject of border security, immigration, and U.S. citizenship compose the bulk of Chapter 9. At the border, there are many challenges and corresponding methodologies to control access. Way beyond fencing alone, the newly developed Customs and Border Patrol (CBP) tackles myriad tasks involving violations of our border integrity. By air and boat, by foot and vehicle, the CBP tracks and traces encroachments. The CBP's involvement with cargo and containers is featured. The last portion of the chapter deals with citizenship and immigration issues, including an assessment of Project Shield, the US-VISIT program, and the Cornerstone Initiative. Added to this edition is a close look at the family separation dilemma, DACA path to citizenship, and the continuing debate over the need or nature of barriers and walls at our borders.

The vast expanse of homeland practice in the airline and transportation industry comprises a major portion of Chapter 10. In an immediate reaction to the Twin Towers attack, DHS set about to establish a series of programs and protocols involving both personnel and equipment. The Transportation Security Agency (TSA) is the center of the activities. Added to their functions would be the federal air marshals, armed officers aboard flights, and the federal flight deck officer program. Using specialized equipment, such as trace portals and biometrics, TSA has been advancing technology across its many duties and responsibilities. TSA continues to struggle with public relation problems with some of its tactics and behavioral failures on the part of select agents. Professionalizing TSA remains a constant concern for policymakers. How Homeland Security practices play out in the maritime world receives considerable attention. From emergency to safety practice, from cargo to ports, the chapter deals with the diverse functions of the U.S. Coast Guard—a crucial player in the world of maritime security. Lastly, the chapter covers how real and mass transit systems must be attentive to homeland demands and features both national, regional, and local rail systems.

The interplay between public health and Homeland Security is the chief aim of Chapter 11. Terrorists' threats are meaningful as to the world's food and water supply. So, too, are the potential harms that can arise from contaminated livestock and poultry. Second, infectious diseases pose an extraordinary threat to the community from a security perspective. The chapter sees a major infusion of data and information on the pandemic COVID 19 and how this plague impacts literally every facet of American life. Special emphasis on mitigation efforts is included but it is clear the pandemic, as of this writing, has a grip on the American and international way of life. How DHS stores antidotes and other medical remedies receives serious attention. A close examination of the National Pharmaceutical Stockpile is part of the chapter's approach, and how a pandemic might impact both individuals and the collective is fully critiqued. Planning documents that address pandemic threats are provided.

The final chapter of the book summarizes a few of the challenges inherent in the task and the natural bureaucracy that emerges in the war on terror. DHS clearly is a work in progress and already has a lively history of change. Some examples of this critical inquiry are: Does DHS grow rationally? Does the mission of DHS match its organizational structure? Has DHS become overly bureaucratic and out of touch? Are the practices of DHS too centralized? Has technology been effectively integrated into the practices of DHS? And has DHS become another political tool for fights and disagreements between our major political parties? Are policymakers in DHS too entrenched to think creatively, or is there a need to think outside normal channels? In the end, I have tried to capture the structure and intent of DHS. The question of what DHS really is may be more metaphysical than we think. All of us can concur on its intent—to make the nation safe. But although we are sure of its intent, it may take a generation or two before we really understand how to shape and construct DHS. For in many ways, DHS mirrors what we are and what we must contend with—a world full of risk and human frailty.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Acknowledgments

The sheer volume of DHS material and content makes this a project that heavily depends on others. To be sure, I could not have authored this alone. Instead, I was heavily dependent on the skill and acumen of colleagues.

To Hope Haywood, my thanks again. I cannot envision being ever able to coordinate this maze of concepts and ideas. In this edition, and all the others, her orchestration of details really leaves me breathless and fully cognizant that these projects would not come into being without people like Hope. She continues to be a master Editor.

To CRC Press, I appreciate the opportunity. Editor Mark Listewnik continues his accessible approach and displays a partnership mentality more than one who merely critiques. Always open to suggestions and forever knowledgeable about our academic discipline and the industry and constituencies we serve, Mark's editorial approach remains unrivaled.

As I enter my tenth year of service at John Jay College, I am forever mindful of my good fortune to labor with academic-scholars and practitioners who engage the system in ways most colleges can only imagine. In addition, I am blessed with excellent departmental colleagues who are supportive and collegial. Lastly, I am continually thankful that John Jay provides resources for scholarship, and this prioritization is largely the result of the leadership of our Provost, Dr. Yi Li and our President Karol Mason.

Part of the John Jay support system relates to the ease in which graduate students are encouraged to work closely with faculty on these types of projects. HS 3rd was blessed to engage Jennifer Bencivenga as a research assistant as she completes her Master's studies. Jennifer's talents were evident from my first day of engagement. With a precise eye and a dedication to doing things with the highest professionalism, Jennifer's contribution to this textbook can only be described as significant. I am deeply appreciative.

In this edition, another graduate student, and now a full-fledged alumnus of John Jay, namely Mashkurul Haque—a former military officer from Bangladesh—made extraordinary contributions to this project. His keen eye and penchant for doing things right and with accuracy were very notable traits. I am very indebted to him for his service.

At home, my blessings simply cannot be counted, for it is family that drives most of what I do. If I leave any legacy to my spouse and closest friend, Jean Marie, and my seven children, it is that their father loved them.

Charles P. Nemeth, JD, PhD, LL.M
Chair and Professor, Security, Fire and Emergency Management



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Author

Charles P. Nemeth, Chair and Professor of Security, Fire and Emergency Management at John Jay College, New York, has spent the vast majority of his professional life in the study and practice of law and justice, the role of private sector justice in a free society, and the ethical demands on justice professionals. A recognized expert on ethics and the legal system, appellate legal practice, and private-sector justice, he also is a prolific writer, having published numerous texts and articles on law and justice throughout his impressive career. His most recent works include these titles: *Private Security and the Investigative Process 3rd* (CRC Press, 2010); *Private Security and the Law*, 4th Edition (Elsevier, 2012) with a 5th edition at (CRC Press, 2017); *Cicero and Aquinas: A Comparative Analysis of Nature and the Natural Law* (Bloomsbury Press, 2017); *Aquinas and King: A Discourse on Civil Disobedience* (Carolina Academic Press, 2010); *Aquinas and Crime* (St. Augustine's Press, 2009); *Criminal Law* (Prentice Hall, 2003; CRC Press, 2011); *Law & Evidence: A Primer for Criminal Justice, Criminology, Law, and Legal Studies* (Prentice Hall, 2001; Jones and Bartlett, 2010); *Aquinas in the Courtroom* (Greenwood and Praeger Publishing, 2001); *Private Sector and Public Safety: A Community Based Approach* (Prentice Hall, 2005); *The Prevention Agency* (California University of Pennsylvania Press—Institute for Law and Public Policy, 2005); and *The Paralegal Resource Manual* (McGraw-Hill, 2008).

An educator for more than 35 years, Dr. Nemeth's distinctive career is a blend of both practice and theory. A member of the Pennsylvania, New York, and North Carolina bars, Dr. Nemeth has extensive experience in all aspects of criminal and civil practice.

His previous academic appointments include Niagara University (1977–1980), the University of Baltimore (1980–1981), Glassboro State College (1981–1986), Waynesburg College (1988–1998), the State University of New York at Brockport (1998–2003), and California University of Pennsylvania (2000–2012). He is a much sought-after legal consultant for security companies on the trend of privatization, and he is a recognized scholar on issues involving law and morality and how ethics relates to the professions.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Introduction

The term “Homeland Security” is of recent invention. For the bulk of this nation’s glorious history, the view that security was inexorably and inevitably tied to the homeland itself was a foreign notion. Surely, the nation always had a continuous interest in the protection of its borders from invasion, and just as assuredly, the nation and its states were perpetually concerned with the protection of the citizenry from natural disasters. To be certain, the idea that government has an obligation to protect and safeguard the citizenry is nothing new under the sun. Yet despite this penchant for safeguarding the general population, protection of the homeland took on a very different meaning in the year 2001. The world changed in more ways than we could have ever envisioned as the attacks on the Twin Towers and the Pentagon unfolded. From September 11, 2001, onward, the world will perceive the idea, the notion of security, and the homeland in a unique and very different way. Homeland Security will be referred to as a “New National Calling.”¹ In *Securing the Homeland: Strengthening the Nation*, President George W. Bush exhorts the citizenry to remember this new vocation:

The higher priority we all now attach to homeland security has already begun to ripple through the land. The Government of the United States has no more important mission than fighting terrorism overseas and securing the homeland from future terrorist attacks. This effort will involve major new programs and significant reforms by the Federal government. But it will also involve new or expanded efforts by State and local governments, private industry, non-governmental organizations, and citizens. By working together we will make our homeland more secure.²

Before 9/11, terrorism was surely one of many variables considered in the planning and implementation of national security. After 9/11, it became the predominant and preeminent criteria in the war on terror and a national fixation in most facets of the public domain.

¹ President George W. Bush, *Securing the Homeland: Strengthening the Nation* (Washington, DC: U.S. Government Printing Office, 2002), 3.

² Bush, *Securing the Homeland*, 3.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

1

The Idea and Origin of Homeland Security

OBJECTIVES

1. To identify major twentieth- and twenty-first-century events, both domestic and international, that formed the United States' current policy position on homeland security
2. To comprehend that war, by its very nature, its military tactics and strategies, and governmental policies, relies on forms of terror to meet its goals
3. To analyze the effect the Cold War had on shaping Americans' notions of terror and to understand the evolution of the government's policy responses
4. To describe the domestic events of the turbulent 1960s and 1970s to shed light on the country's response to domestic terrorism as well as gain an understanding of the unique motivations of the domestic terrorist
5. To differentiate the motives of the international terrorist from the domestic terrorist and comprehend that although the methods may be the same, the motivations differ
6. To explain the unique motivations of the jihadist by exploring attacks against U.S. military targets and discover the motivations leading up to the events of 9/11
7. To evaluate specific international terror incidents against U.S. installations prior to 9/11 to gain an understanding of the jihadist mentality that led up to the terror attacks against the Twin Towers and the Pentagon
8. To identify specific domestic terror attacks, such as those perpetrated by Timothy McVeigh and Ted Kaczynski, the Tree of Life-Pittsburgh Synagogue Shooter, by way of examples, in light of the effect these types of attacks have on national security policy

1.1 Introduction

The concept of a threat to the homeland has historically taken many shapes. Terror and the terrorist are not new phenomena—they are a construction of the ages, seen throughout history

Homeland Security

in various guises. In recent years, the country has focused on domestic security and preventing acts of terrorism. The new domestic terrorist continues to evolve, whether driven by racial, religious, or ideological motives, from the left or the right, or “planted” among us—a trained and brain-washed actor determined to cause havoc. In short, we are under stress from within and without. As we move toward a twentieth year reflection on the events of 9/11, it is clear that domestic terrorism has unfortunately grown in scope and size, whether it be driven by racial or ethnic hatred, religious bigotry, or extreme ideologies like supremacy or environmental issues.¹ Couple this perspective with a predictable national desire to protect one’s homeland, and nothing here is unexpected. What is of greater utility in the discussion of security of the homeland will be how we arrived at our current position. Specifically, what did we do before the jihadist? What types of terror attacks did America experience? What motivated the terrorist? For example, the Ku Klux Klansman is hardly a jihadist, although his methods may be just as dastardly. How do we reconcile that difference, or is there really a difference at all when measuring harm? In fact, the crazed shooter who enters religious settings, whether mosque, church, or synagogue, operates from just as extreme an ideology as the jihadist. What of the military dictator, the tyrant, the leader who leads his country to ruin and grounds his enterprise on hate, such as the leader of the Third Reich? This too is terror by any reasonable definition. Terror is nothing new, although terror adopts new rationales, new causes, and new methodologies.

The acts of the terrorist have been with us since the dawn of recorded history. It is important to keep this in context in our interpretation of history. This chapter traces a whole host of acts and movements in the twentieth century that preceded the events of 9/11. All the examples covered illuminate how and why terrorists do what they do. All these illustrations, from the military machine that oppresses people and states to the radical protest groups, like the “Weathermen” who sabotage government installations, help to bring perspective to the discussion. When one scrutinizes the diversity of these acts and approaches, one can better understand the landscape of modern terrorism in a post-9/11 world.

1.2 Threats to the Homeland: Twentieth-Century Military Movements

While much can be written about the nature of threat and violence throughout U.S. history, the best place to start in order to understand modern-day terrorism is the twentieth century—a century with complex conflicts and territorial challenges. From World War I (WWI) to World War II (WWII), the concept of threats to the homeland was largely the result of country-to-country conquests, political disagreements, and imperial empire building. For example, the Third Reich’s move across the Polish frontier, in the name of the reclamation of Aryan races under the thumb of the Polish authorities, is a land grab with a eugenic flavor. This is a very different kind of threat from that currently considered by the Department of Homeland Security. Yet, these wars and conflicts serve as an appropriate backdrop for the way any nation seeks to maintain its territorial integrity. In a sense, the planes attacking the World Trade Center buildings were an assault on the country’s sovereignty not unlike the way the German troops crossed into the Sudetenland (Figure 1.1).

The means and motivation are clearly different, though the net effect is not completely dissimilar. The Nazi onslaught of WWII was, in a sense, the largest whole-scale terror campaign ever inflicted on a continent (Figure 1.2).

Aside from this illegal and unjustified sweep of countries, Germany culminated its terror by implementing its Final Solution, its programs of extermination of Jews and all forms of resisters, of the mentally disabled, the old and infirm, homosexuals, Rabbis, Catholic priests, and Lutheran ministers. More than six million human beings perished under the crush of an evil state (Figure 1.3).

1.2 Threats to the Homeland: Twentieth-Century Military Movements



Figure 1.1 German troops goose step through Warsaw, Poland, during the 1939 invasion that saw Poland fall within 3 weeks. The invasion caused Britain and France to declare war on Germany. (From National Archives, image 200-SFF-52.)

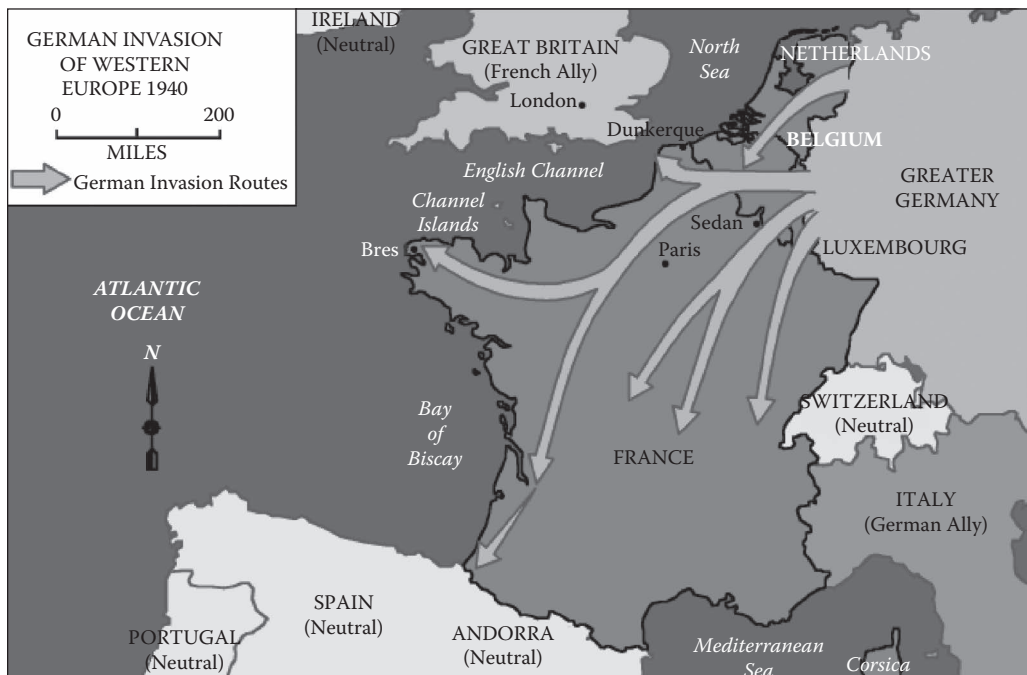


Figure 1.2 From Poland to Stalingrad, from Holland to Northern Africa, the propaganda of the Third Reich was a campaign that terrorized the entire civilized world. (Courtesy of the U.S. Holocaust Museum, Washington, DC.)

That the Nazi regime engaged in deliberate, intentional threats against whole races, ethnic types, and classifications of citizens is a self-evident conclusion when the historical record is scratched just a little. The systematic extermination program was the subject of endless meetings and conferences, though admittedly the Nazi leaders were quite effective in removing the paper trail. In 1942, at what was billed as the Wannsee Conference, the leadership of the Schutzstaffel (SS) and the Nazi and other aligned government entities met to discuss the efficacy and corresponding efficiencies of mass extermination. Leading the charge calling for the physical extermination of millions was SS officer Reinhard Heydrich (Figure 1.4).



Figure 1.3 A survivor stokes smoldering human remains in a crematorium oven that is still lit, Dachau, Germany, April 29–May 1, 1945. (Courtesy of the U.S. Holocaust Museum, Washington, DC.)



Figure 1.4 Reinhard Heydrich, chief of the SD (Security Service) and Nazi governor of Bohemia and Moravia. Place uncertain, 1942. (From National Archives and Records Administration, College Park, MD.)

The bureaucratic apparatus was coupled with legions of resources, from transportation to the building of crematoria. The task of moving millions of people to their own deaths required extraordinary efforts by the captains of industry. Consider the complexities of rail movement alone as portrayed in Figure 1.5.

1.2 Threats to the Homeland: Twentieth-Century Military Movements

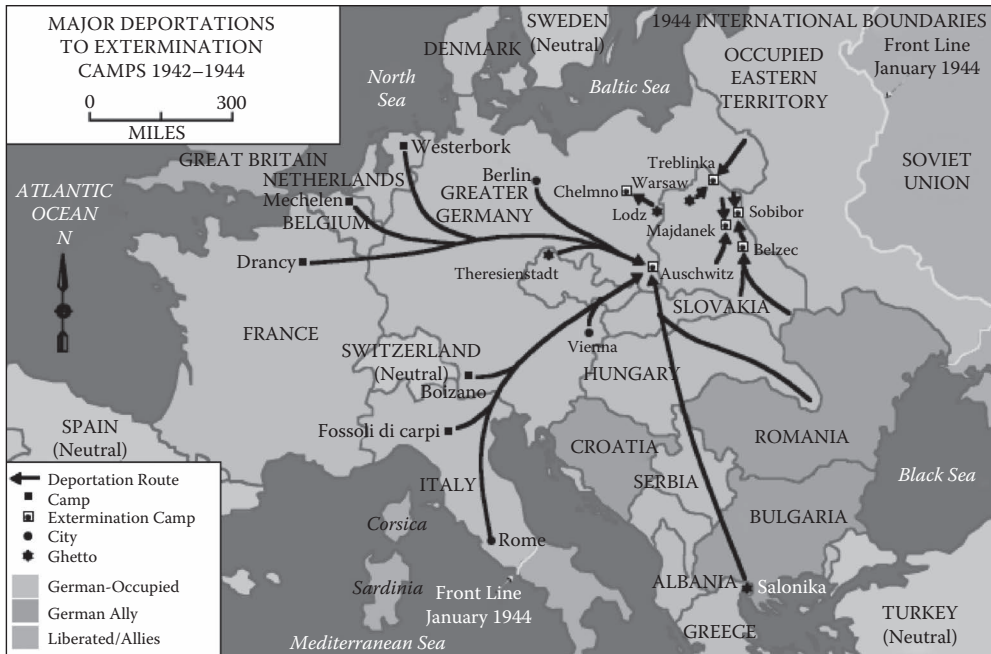


Figure 1.5 The Germans attempted to disguise their intentions, referring to deportations as “resettlement to the east.” The victims were told they were to be taken to labor camps, but in reality, from 1942 onward, deportation for most Jews meant transit to killing centers and then death. (Courtesy of the U.S Holocaust Museum, Washington, DC.)

Similar arguments about Japanese imperialism can be posited and for good reason. The Japanese intent was to dominate and rule the world using means far outside the mainstream of modern warfare. The survivors of the Japanese occupation of the Philippines or of Japan’s own concentration camps tell a story of brutality and degradation that seems inexplicable when one considers the modern democratic state of Japan. The notorious Unit 731 on the Japanese mainland witnessed forced sterilization, castration, live burial, vivisection, mutilation, and mass experimentation (Figure 1.6).

Internet Exercise: Visit [Unit 731.org](https://unit731.org)—a web location dedicated to advancing the truth about this horrid place especially considering its notorious biological experimentation—at: <https://unit731.org>.

None of these atrocities can be adequately covered in a text on homeland security, although it is critical that the reader understands that war, by its very nature, depends on terror to some extent. Whether it is the summary execution of civilians and prisoners of war or the indiscriminate bombing of wholesale populations, terror is both an end and a by-product of war. Much of what we witness in the terror battlefield today connects its heritage to the makings and doings of war. By way of illustration, Saddam Hussein thought Joseph Stalin—one of history’s most remarkable figures—was to be envied and copied in his approach. Under the guise of “re-education” and resettlement, a technique mastered by the Nazi regime, even contemporary foreign powers employ similar tactics regarding special populations. China, by way of illustration, herds Muslims into a system of Gulags—with some estimates being in the millions, just because these individuals are Muslim.² See Figure 1.7.³

If anything is true about historical trends and events, it is their undeniable repetition and for this reason alone, the past always illuminates the future. In this way, a look at twentieth-century conflicts can illuminate the rationale behind the tactics used by terrorists.



Figure 1.6 Camp 731 beheading an American POW. (Courtesy of the University of Minnesota, Center for the Study of Holocaust and Genocide Studies.)



Figure 1.7 Re-education Center for Muslims in Mainland China at Dabancheng in April 2018. (Courtesy of Google Earth.)

1.3 Threats to the Homeland: The Cold War Experience

At the end of the conflagration known as WWII, another conflict of a very different sort emerged—the Cold War. As the victors of WWII set out to fashion a new Europe and continental framework, the Allies saw the world in distinct and sometimes incompatible ways. For sure, Britain and the United States shared the core values of freedom and democratic, republican principles. By contrast was the starkly divisive approach of our Russian ally, whose Trotskyite–Leninist revolutionary mindset was fundamentally at odds with Western ideals. The Russian mindset struck directly at the heart of free societies. At the end of the war, during the Potsdam Convention, Russia’s expansionist desires clearly won the day (Figure 1.8).

1.3 Threats to the Homeland: The Cold War Experience

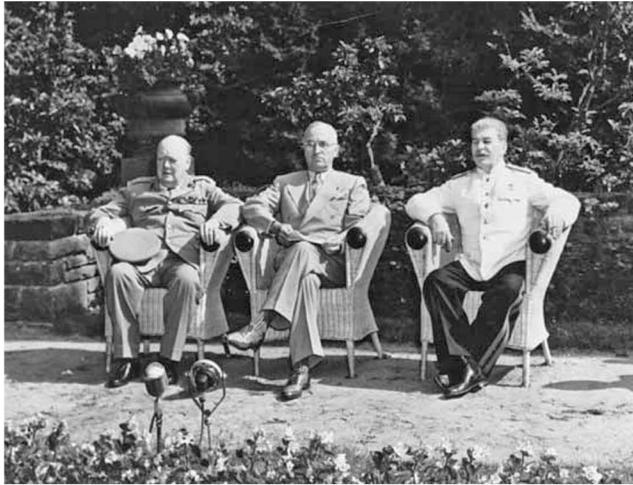


Figure 1.8 Churchill, Truman, and Stalin during the Potsdam Convention. (Courtesy of the Truman Library.)

Dividing up countries such as Germany and replacing the system in free democratic or monarchical countries such as Poland and Hungary with a Soviet-style socialist model, the Russian Bear flexed extraordinary muscle immediately after the end of the conflict. Concession after concession was made to the Soviet demand, much to the distress of Winston Churchill.

In response, Churchill ultimately sounded a clarion call for halting the expansion of the Soviet empire in one of his finest speeches.⁴

I have a strong admiration and regard for the valiant Russian people and for my wartime comrade, Marshal Stalin. There is deep sympathy and goodwill in Britain—and I doubt not here also—toward the peoples of all the Russias and a resolve to persevere through many differences and rebuffs in establishing lasting friendships.

It is my duty, however, to place before you certain facts about the present position in Europe.

From Stettin in the Baltic to Trieste in the Adriatic an iron curtain has descended across the Continent. Behind that line lie all the capitals of the ancient states of Central and Eastern Europe. Warsaw, Berlin, Prague, Vienna, Budapest, Belgrade, Bucharest and Sofia; all these famous cities and the populations around them lie in what I must call the Soviet sphere, and all are subject, in one form or another, not only to Soviet influence but to a very high and in some cases increasing measure of control from Moscow.

Internet Exercise: To read Churchill's entire speech, titled "The Sinews of Peace," visit http://www.nato.int/docu/speech/1946/S460305a_e.htm.

By 1946, Churchill knew full well that a geopolitical shift was underway. In appealing to the United States, he urged its government to consider its many sacrifices of men and material and to envision a world where an "iron curtain" would split the free from the oppressed. He argued that the legacy of the sacrifice must amount to more than an iron wall between the totalitarian and the democratic. But this is exactly what was unfolding and with frightening speed—a new world order divided in two and directly at odds with one another. Hence, a new war emerged—one not fought on the battlefield but in the sphere of territorial conquest and subliminal and direct attempts to destroy either side. This is the stuff of the Cold War, and it escalated very quickly. The United States quickly recognized these expansionist motivations. And this sort of expansionist mentality is nothing new nor has it evaporated from the current terror scene. The Islamic State of Iraq and Syria (ISIS), the contemporary Islamic state group, also known as the Islamic State of Iraq and the Levant (ISIL), operates based on a similar mentality.⁵



Figure 1.9 Military base at Perevalne during the 2014 Crimean crisis. (Photo by Anton Holoborodko shared under a CC BY-SA 3.0 license. March 8, 2014, available at https://commons.wikimedia.org/wiki/File:2014-03-09_-_Perevalne_military_base_-_0162.JPG.)

Internet Exercise: Read President Harry Truman’s Secretary of State Keenan’s letter to General George C. Marshall for his prescient commentary on an upcoming Cold War at www.trumanlibrary.org. Click on *Online Collections* in the Library Collections menu, then click on *Ideological Foundations of the Cold War* under “Research Files,” then under *1946*, locate the January 29, 1946, telegram from George Kennan to James Byrnes.

The Cold War was not an illusory war by any means but one with significant military and political consequences. By 1947, the Soviet Union commenced the construction of the Berlin Wall—separating the East from the West and trapping East Berlin in a dark, communist world. Ever the expansionist, the Soviet Union boldly expanded its sphere of influence into countries such as Iran. Some would argue that the Cold War has recently re-emerged with Russian incursions into the Crimea, into the Ukraine, and other aggressive postures, which signify this expansionist mentality. See Figure 1.9.

In the wake of these actions, President Harry Truman discerned a meaningful and bona fide threat to free peoples. As a result, he made plain that the United States would not sit idly by while Soviet aggression spread throughout the world. In 1947, Truman enunciated what is now known as the Truman doctrine. With the Truman doctrine, President Truman established that the United States would provide political, military, and economic assistance to all democratic nations under threat from external or internal authoritarian forces. The Truman doctrine effectively reoriented U.S. foreign policy, guiding it away from the usual stance of withdrawal from regional conflicts not directly involving the United States to one of possible interventions in faraway conflicts.

Internet Exercise: Browse through the Truman Library online collection relating to the Truman Doctrine at <https://www.trumanlibrary.gov/library/online-collections/truman-doctrine>.

In light of the Soviet Union’s development of an atomic bomb in 1949, the doctrine was never more important to fend off threats to our national security. See Figure 1.10 for a timeline of the Cold War to the point of Soviet nuclear power.

With the emergence of the Cold War, relations between the Western nations and the Soviet Union spiraled in a downward fashion for years afterward. The first major test of this tension was manifest in the Berlin Airlift of 1948–1949, when supplies for beleaguered Germans were dropped daily, over objections from Soviet officials who had set up blockades to thwart the delivery of much-needed supplies. The Soviets also closed roads and forbade movement from one sector of the city of Berlin to the other. The western edge of Berlin largely remained in American/British hands,

1.3 Threats to the Homeland: The Cold War Experience

Timeline of the Cold War - 1945-1949
1945-1946: Creation of Eastern European People's Republics
1946: George Kennan's Long Telegram and the Policy of Containment
1946: Churchill's Iron Curtain Speech
1946: Soviet Troops in Iran
1947: Truman Doctrine
1947: U.S. Efforts to Control Atomic Energy
1947: Marshall's Offer of Economic Assistance
1948-1949: Berlin Airlift
1949: North Atlantic Treaty Organization
1949: Creation of the two Germanys
1949: Soviet Atomic Bomb

Figure 1.10 Timeline of the Cold War: 1945–1949.

while the smaller northeastern portion of Germany remained Soviet. The Soviets were figuratively choking the people of Berlin. U.S. C-47s began a mass supply line to overcome this obstacle. The planes flew in three major corridors toward the city (Figure 1.11).

When the Soviet Union entered a treaty with China, the geopolitical framework of the world stood on its historic head. As Soviet expansionism marched onward, the United States felt obliged to “save” free peoples or, when the nations were not all that free, to keep the flow of communism to a bare minimum.

Throughout the 1950s, the problems associated with the Cold War worsened. Nuclear proliferation, uprisings in Soviet-dominated countries, human rights violations without precedent, and a host of other evils heaped on unwilling populations—all signify the tragedy and the worst elements of communism in practice. The major events of the Cold War during the 1950s are outlined in Figure 1.12.



Figure 1.11 Berlin Airlift at Tempelhof Airport. (Courtesy of the Truman Library.)

THE TIMELINE OF THE COLD WAR - 1950-1959
1950: Sino-Soviet Treaty
1950: NSC-68
1950-1953: Korean War
1952: U.S. Hydrogen Bomb
1953: Stalin's Death
1953: Soviet Hydrogen Bomb
1954: Atomic Energy Act
1955: Creation of the Warsaw Pact
1955: Austrian State Treaty
1955: Big Four Geneva Summit
1956: Twentieth Congress of Soviet Communist Party
1956: Polish Uprising
1956: Suez Crisis
1956: Hungarian Uprising
1957-1958: Sputnik and the Space Race
1958: Suspension of Nuclear Tests
1958: Khrushchev's Berlin Demands
1959: Khrushchev Visits the United States
1959: Khrushchev-Eisenhower Meeting at Camp David
1959: Antarctic Treaty

Figure 1.12 The Timeline of The Cold War: 1950–1959.

Of course, the Truman doctrine was cited in the Korean War, the Cuban Missile Crisis, and the Vietnam War. When President Kennedy confronted the Soviet government for its dispatch of long-range missiles to Cuba (Figure 1.13), the justification was the containment theory, the right of the Western hemisphere to be safe from this corrupt hegemony, and the insistence of Harry Truman that free peoples need not tolerate this political oppression.

Each of these unofficial wars was, at least in a legislative sense, an effort to contain the “threat” of communist takeover. Throughout the 1960s and 1970s and into the early 1980s, the two opposing giants in the Soviet and American systems remained entrenched. Nuclear proliferation continued unabated. A lack of trust and cooperation remained standard operating procedures. Spy agencies, such as the Central Intelligence Agency (CIA) and the Soviet Committee for State Security, the KGB, spent most of their energy engaged in the activities and efforts of the Cold War.

When President Richard Nixon visited China in 1972 (Figure 1.14), a tectonic shift occurred in the Cold War. Nixon had brilliantly undercut the Sino-Soviet cooperation that had appeared impenetrable for so many generations. Nixon made possible a new vision of cooperation on missile deployment, cultural exchange, and foreign relations.

1.3 Threats to the Homeland: The Cold War Experience



Figure 1.13 U-2 reconnaissance photo showing concrete evidence of missile assembly in Cuba. Shown here are missile transporters and missile-ready tents where fueling and maintenance took place. (Courtesy of the CIA.)

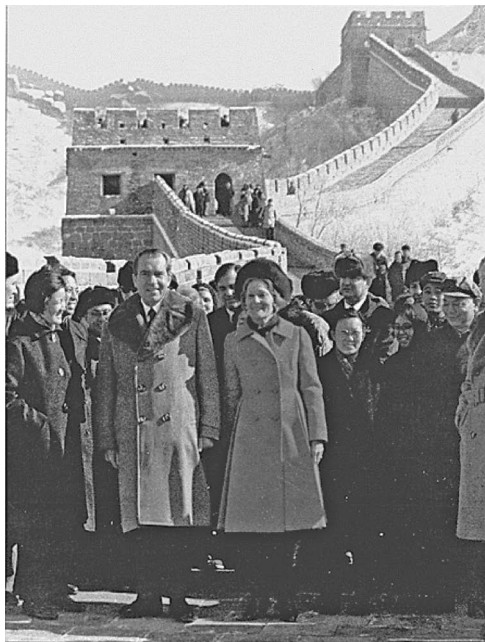


Figure 1.14 President and Mrs. Nixon visit the Great Wall of China and the Ming tombs, February 24, 1972. (Courtesy of the National Archives.)

From this point onward, the Soviet system would be isolated and suffered internally from decades of misplaced investment in the military model over any other benefit for its people. The Soviet system was crumbling from within. By the time of President Ronald Reagan, the time was ripe for an end to the intolerable Cold War (Figure 1.15).



Figure 1.15 Ronald Reagan at the Brandenburg Gate, Berlin, Germany, June 12, 1987. (Courtesy of the Ronald Reagan Library.)

Reagan was an unabashed believer in the American way of life. He showed diplomacy in the background of negotiations and protocol, but publicly there was no greater critic of the Soviet system. On March 8, 1983, when he labeled the Soviet state an “evil empire,” critics charged him with sensationalism. Those who supported Reagan felt that he was defending the notion of freedom, believing that any government that dominated and oppressed its people was unjust in the eyes of history and its people. He was a strong proponent for the elimination of communism and, in particular, the Soviet-style system. This tendency to label repressive governments as “evil” continues even to the present with certain countries designated the “Axis of Evil” whose membership includes Iran and North Korea though some might firmly include Russian and China in this mix.⁶ Prescient in Reagan’s position on Soviet-style communism and his belief that it would ultimately fall, he remarked:

In the 1950s, Khrushchev predicted: “We will bury you.” But in the West today, we see a free world that has achieved a level of prosperity and well-being unprecedented in all human history. In the Communist world, we see failure, technological backwardness, declining standards of health, even want of the most basic kind—too little food. Even today, the Soviet Union still cannot feed itself. After these four decades, then, there stands before the entire world one great and inescapable conclusion: Freedom leads to prosperity. Freedom replaces the ancient hatreds among the nations with comity and peace. Freedom is the victor.

And now the Soviets themselves may, in a limited way, be coming to understand the importance of freedom. We hear much from Moscow about a new policy of reform and openness. Some political prisoners have been released. Certain foreign news broadcasts are no longer being jammed. Some economic enterprises have been permitted to operate with greater freedom from state control.⁷

Reagan was often labelled a dreamer, an idealist lacking common sense, and worst of all, an “actor.” However, while no administration is perfect, he was consistent in his approach. Ultimately, it was his interpersonal skill and relationship with Mikhail Gorbachev that set the stage for much that followed—among other things, the fall of the Berlin Wall and, subsequently, an end to the Cold War. Threats that had generated so much fear were replaced with cautious friendship. There is something to be learned from this episode in history. Just as the Russians were deemed the ultimate threat to the United States, so too is the terrorist extremist currently considered the most immediate threat.

To be sure, both have been at the forefront of our national security over the years. What we do know is that enemies are not permanent stations. They are subject to change. Experts at the time would never have imagined the United States and Russia having closer ties and working

1.3 Threats to the Homeland: The Cold War Experience

together. Yet, the two countries have taken many diplomatic strides, though it is too early to tell with the current political leaders in Russia with the re-emergence of Vladimir Putin. Putin is often referred to as Russia's strongman, and he works arduously to develop this caricature among his countrymen.⁸ Putin has been vocal and transparent in many of his efforts to consolidate power, although Russia is not the nation once ruled by the KGB but a populace that has tasted some aspects of a free society. The mass demonstrations of December 2011 say much about a Russian political system evolving (Figure 1.16).

While only time will tell in the matter of Russian political processes, it is a safe bet that once the citizenry experiences a bit of freedom, there will be no going back. It seems the prospect of improved Russian-U.S. relations appears on hold at present. There is Russia's military intervention in Ukraine. See Figure 1.17.

Current foreign policy decisions regarding the Middle East, especially in regard to Syria, were once thought to be a door opener for better relations.⁹ Unfortunately, in Syria, U.S. hesitancy to get involved coupled with Russian intervention has triggered the possibility of a new cold era. The Iran nuclear agreement and the Russian–Iranian partnership have also fueled tension, along with rising distrust.



Figure 1.16 Demonstrators hold Russian opposition flags in Nizhny Novgorod. Anti-Corruption Rally (26 March 2017). Creative Commons (CC BY-SA 4.0).



Figure 1.17 Vladimir Putin. (Courtesy of Presidential Executive Office 2020. Creative Commons Attribution 4.0 International. <http://en.kremlin.ru/press/photo>.)

1.4 Threats to the Homeland: Iran, Terror, and the World Stage

It is difficult to imagine how long the United States has been entangled with the Iranian regime over the last 50 years—and most of that relationship has been strikingly negative and undergirding this tension has been the Iranian ties to terror as a means to political and social change. Iran's colonialized history, formerly under British rule, and then eventually under a less than perfect monarchy of the Shah of Iran until the Islamic revolution of 1979, was less dedicated to terror than it presently was and is. See Figure 1.18.

During the Presidency of Jimmy Carter, the U.S. Embassy in Tehran was taken over by Islamic radicals who kept American staff and employees hostage for 444 days—while overthrowing the Shah and replacing him with a theocratic state of Islamic Mullahs who to this day lead the country. So troubling was this seizure that most political observers on presidential politics conclude that the rise of Ronald Reagan was directly tied to what was perceived as military impotence under the leadership of President Carter.¹⁰ See Figure 1.19.

Iran is an ongoing saga for the United States, and since the capture of the U.S. Embassy the relationship has never been positive. In fact, the United States sees and characterizes the Islamic State of Iran as a direct supporter and supplier of terrorism across the world. Even to the present day, the United States has applied economic and political sanctions against the regime.¹¹

While some may debate this position as extreme, it is clear that Iran has funded and supported terror activities even to the point of being major suppliers of IED's that directly kill American forces in Afghanistan and Iraq. In 1984, the U.S. State Department designated Iran as a "State Sponsor of Terror." The list of terroristic activities is corroborated and confirmed especially through groups like Hezbollah, supported and supplied by Iran but placed in neighboring countries like Lebanon. Iranian tentacles of terror have been evident throughout the Middle East and as part of its efforts to Islamize the entire region and drive out cultures and entities that do not directly mirror the Mullah's outlook (Figure 1.20).^{12,13}



Figure 1.18 Jimmy Carter speaks at a State Dinner hosted by the Shah of Iran. 12/31/1977. President Carter, center, to right, the Shah of Iran. (Courtesy of The Carter Library <https://commons.wikimedia.org/wiki/File:ShahCarter.gif>.)

1.4 Threats to the Homeland: Iran, Terror, and the World Stage



Figure 1.19 Crowds rush the gate at the U.S. Embassy in Tehran on November 4, 1979. (Courtesy of <https://nsarchive.gwu.edu/briefing-book/iran/2019-11-04/1979-iran-hostage-crisis-recalled>.)

And the entire approach which underpins the Islamic State and corresponding revolution is political to be sure but even more dangerously, highly ideological, highly self-justified by its own theocratic mentality of righteousness. DHS sees the Iranian threat targeting the values and ideals of Western culture. Those targets are graphically portrayed in Figure 1.21.¹⁴

Nothing can edify this negative reality more than the persecution of Christians in the region—the program often being labelled a form of intentional genocide.¹⁵ Even our long-standing ally, Turkey, has been accused of being part of this alienation and persecution of Christian minorities in the region.

What is clear is how terror evolves in this very troubled part of the world—from the 1979 Islamic takeover of the American embassy in Tehran to the development of counter military arms of these states to defend against “invasion” by foreign elements, from Russia’s Afghanistan incursion to the United States nearly 20-year war in Iraq and Afghanistan. In reaction, Al Qaeda formed to counter the invading forces and to engage in a war rooted in the terroristic, asymmetrical model of operation. ISIL/ISIS—the Islamic state group dedicated to carrying out the Caliphate for world domination further illustrates the wide-sweeping influence of these terror groups.¹⁶ Figure 1.22¹⁷ charts the growth and influence of these various groups throughout the world.

For a timeline of these diverse groups dedicated to spreading the Islamic revolution, see Figure 1.23.¹⁸

Internet Exercise: See Chapter 5 in the following report, a U.S State Department set of links to every imaginable set of foreign terrorist organizations, at: <https://www.state.gov/reports/country-reports-on-terrorism-2018/>

ISIS, once dominant in many parts of the Middle East, has been reduced to a minor influence by the effective and relentless attacks by the U.S. and its Coalition forces.

Extracting the United States from these complex campaigns, from Syria to Afghanistan, had been a priority of former President Donald Trump, although effecting a removal is always easier said than done. In Syria, the mass casualties of the country’s overall population have been distressing to say the least. See Figure 1.24.¹⁹

A HISTORY OF IRANIAN ATTACKS ON AMERICANS

For almost four decades, Iran and its terrorist proxies have targeted American civilians and military personnel. From the 1983 bombing of the U.S. Marine barracks in Beirut to more than a decade of attacks against U.S. military personnel in Iraq, Iran's terrorist proxies have killed more Americans than any terrorist group other than al-Qaida. These attacks underscore Iran's malign activities in the region and beyond. Congress and the administration must continue to confront Iran's regional aggression and support for terrorism.



HOSTAGES HELD AT U.S. EMBASSY IN IRAN

A group of Iranian students backed by Islamic Revolutionary leader Ayatollah Khomeini took control of the U.S. Embassy in Tehran, holding 52 U.S. diplomats and citizens hostage for 444 days.



SUICIDE BOMBINGS IN LEBANON

The Iranian-backed terrorist organization Hezbollah—founded, armed, trained and funded by Iran—conducted two suicide bombings in Lebanon: the April bombing of the U.S. Embassy in Beirut killed 17 Americans and the October bombing of the U.S. Marine barracks in Beirut killed 241 Americans.



MINE ATTACK IN THE PERSIAN GULF

Iran—in violation of international law—mined the Persian Gulf. In 1988, one such mine struck the U.S. Navy guided missile frigate USS Samuel B. Roberts, injuring 10 sailors and blowing a 15-foot hole in the vessel's hull.



TRUCK BOMBING IN SAUDI ARABIA

Hezbollah terrorists—with Iranian backing and support—attacked U.S. military forces housed in the Khobar Towers in Dhahran, Saudi Arabia, killing 19 Americans and wounding 372.



SUPPORT FOR 9/11 HIJACKERS

Iran knowingly permitted members of al-Qaida, including several of the 9/11 hijackers, to transit Iranian territory on their way to Afghanistan for training. In April 2018, a U.S. judge ordered Iran to pay \$6 billion to the families of 9/11 victims for supporting the hijackers.



DEADLY IRANIAN INFLUENCE IN IRAQ

Iranian-backed Shiite militias in Iraq killed hundreds of U.S. service members and civilians. Iran provided training and material support for repeated attacks on U.S. personnel with conventional weapons and missiles, as well as sophisticated improvised explosive devices (IEDs) and explosively formed projectiles (EFPs).

www.aipac.org

Figure 1.20 History of Iranian Attacks on Americans, 1979–2018.

(Continued)

1.4 Threats to the Homeland: Iran, Terror, and the World Stage

A HISTORY OF IRANIAN ATTACKS ON AMERICANS



UNJUSTLY DETAINING AMERICANS

Iran has imprisoned U.S. citizens on spurious charges and without due process for decades. Former FBI agent Bob Levinson has not been heard from since he was arrested in Iran in 2007.



ASSASSINATION ATTEMPT IN D.C.

American law enforcement disrupted a plot backed by Iran's Islamic Revolutionary Guard Corps (IRGC) to assassinate the Saudi Arabian ambassador to the U.S. by bombing a popular restaurant in Washington, D.C.



ATTACKS ON U.S. INTERESTS IN AFRICA

Members of the IRGC in Nigeria were arrested for planning bombings targeting American- and other Western-affiliated destinations in the country.



HARASSMENT IN THE PERSIAN GULF

Iran's military has repeatedly taken a range of provocative actions against Americans in international waters, including charging American ships at close range as well as the seizure of two naval vessels and 10 U.S. sailors in January 2016.



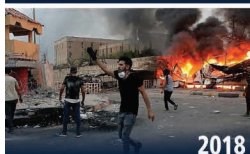
HEZBOLLAH PLOTS ATTACKS IN U.S.

In June 2017, two Hezbollah operatives were arrested for conducting surveillance of U.S. military and law enforcement facilities, as well as airports, in New York City in preparation for terrorist attacks against Americans.



AGENTS OF IRAN IN THE U.S.

In August 2018, two Iranian agents were arrested for surveilling potential terrorist targets in the United States, including Israeli and Jewish targets in Chicago.



IRANIAN PROXIES TARGET U.S. DIPLOMATS

Iranian-backed terrorist proxies in Iraq launched attacks against the U.S. Embassy in Baghdad and the U.S. Consulate in Basra. The funding and training for these assaults came directly from Iran.



OCTOBER 2018

Figure 1.20 (CONTINUED) History of Iranian Attacks on Americans, 1979–2018.

Homeland Security



Figure 1.21 Terrorism key target types.

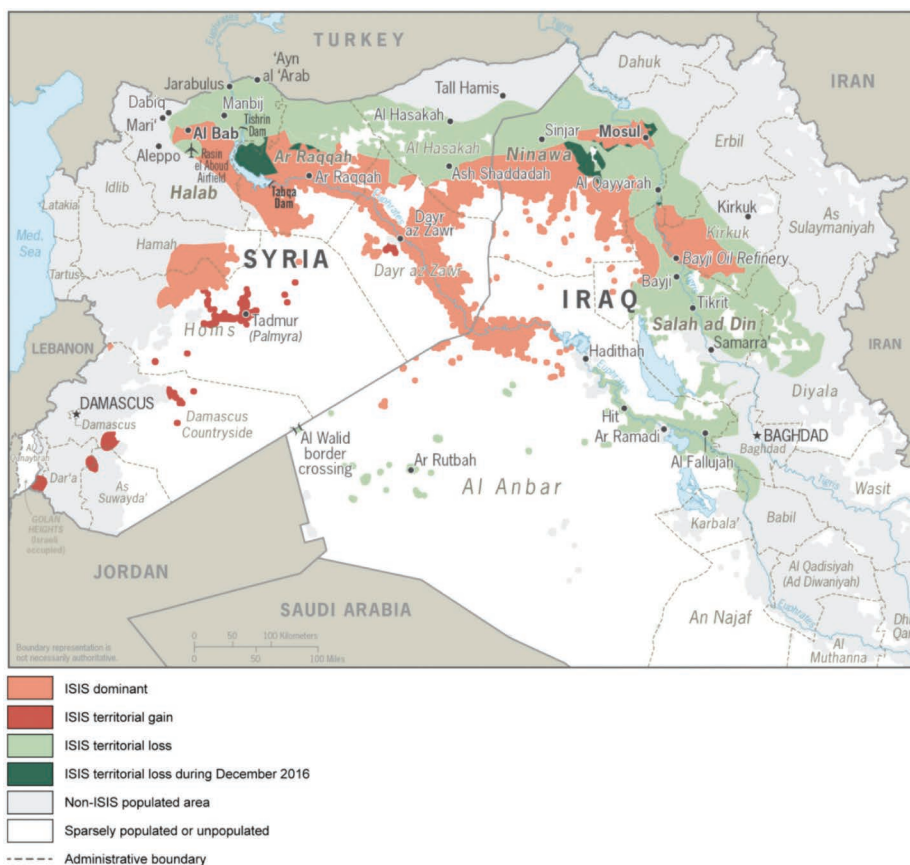


Figure 1.22 Growth of Islamic terrorist groups.

1.5 Threats to the Homeland: North Korea: An Old and New Enemy in the War on Terror

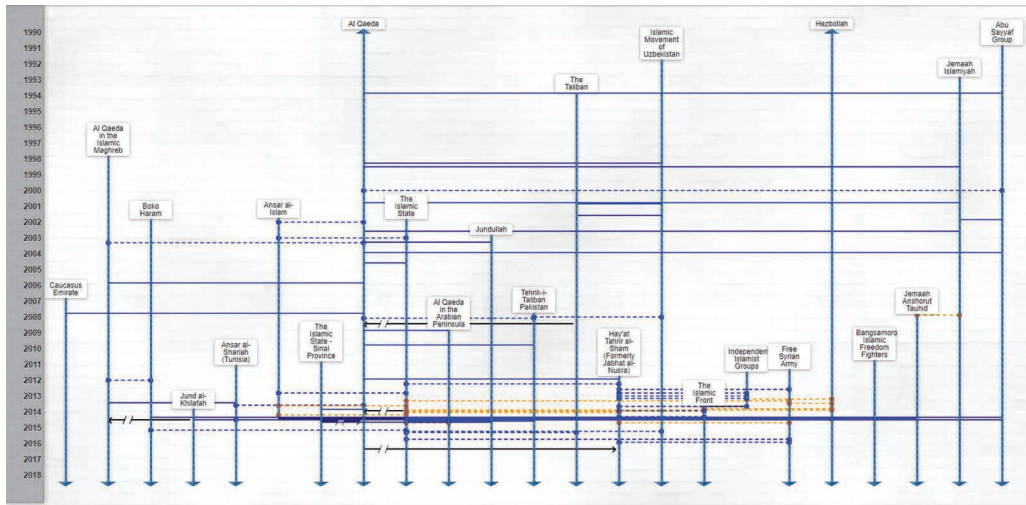


Figure 1.23 Timeline of Islamic terrorism groups.

Death Count in Syria: 450,000 – Children: 50,000

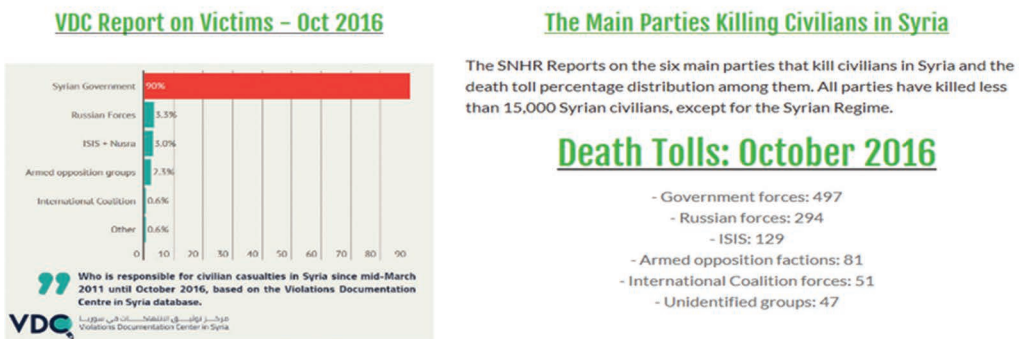


Figure 1.24 Sources differ on Syrian death toll figures.

1.5 Threats to the Homeland: North Korea: An Old and New Enemy in the War on Terror

Recently to the forefront in the world of terror has been the sharp return of North Korea and its leader Kim Jong-Un. Kim merely continues what has been a long-standing hostility to the West since the Korean War. At present, the “Hermit Kingdom” continues its dangerous gambit in the world of nuclear weapons despite repeated condemnations by world leaders and even the United Nations.²⁰ See Figure 1.25.²¹

North Korea has long been under the influence of China and its Communist Party as well as having strong relationships with other Communist governmental authorities such as the Soviet Union and Cuba. It has been separated from its other half—South Korea—which has been a thriving democratic state and an equally thriving capitalist economic system. This tension has continued since the early 1950s. Its ruling class and governmental structure have largely been



Figure 1.25 Map of North and South Korea.

the province of the “Kim” family since the turn of the twentieth century—with three distinct “Dear Leaders” ruling over a country suffering from all sorts of ills. See Figure 1.26.²²

North Korea has a well-documented series of food shortages that have caused or triggered mass starvation in the country as well as limited life spans when compared to its southern counterpart. Its economic system simply cannot and does not provide for its people and efforts to launch the country into market reforms are largely futile, and the comparison with its southern sister could not be starker.²³

North Korea’s extreme isolationism and nearly 70-year history living in a demilitarized zone separating itself from not only South Korea, but the rest of the world, should always give pause to those concerned about terror and warfare in the modern age. The relationship to other terror states also causes continuous concerns for professionals in homeland security for in order to supply basic needs for the country, North Korea enters bargains with rogue nations to fuel its continued existence. Iran, by way of example, has increased its ties to North Korea especially in regards to arms sales.²⁴ And there is little question that the United States, its military branches, and the Department of Defense never discount this country but instead are always preparing for a potential conflict.²⁵

While North Korea remains a terror threat to its neighbors, especially Japan and South Korea, the last few years have witnessed an interesting thaw in this once cold relationship. Aside from the meeting of former President Trump at the Demilitarized Zone, the nation has been engaged in bilateral negotiations with the United States and has largely ceased its once regular firing of ballistic missiles. See Figure 1.27.

1.5 Threats to the Homeland: North Korea: An Old and New Enemy in the War on Terror

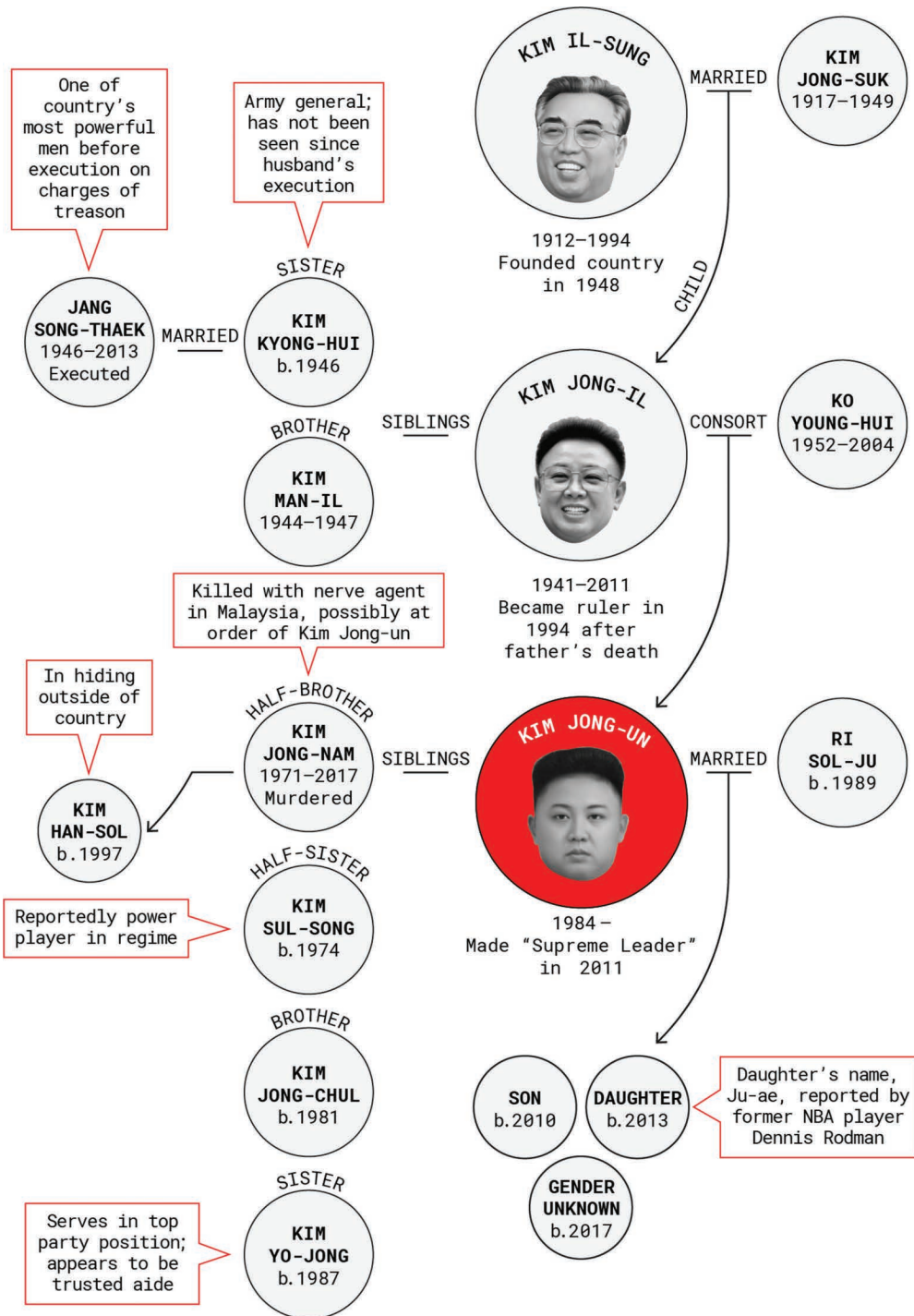


Figure 1.26 All in the family—three generations of Kims: A selective history. North Korea's secrecy makes it difficult to verify information about Kim Jong-un's children, including how many there are and when they were born. His wife's birth date is also unconfirmed. (Courtesy of the Brookings Institution.)



Figure 1.27 President Donald J. Trump shakes hands with Chairman of the Workers' Party of Korea Kim Jong Un Sunday, June 30, 2019, as the two leaders meet at the Korean Demilitarized Zone. (Official White House Photo by Shealah Craighead.)

1.6 Threats to the Homeland: Revolution, Riot, and Rightful Demonstration

There is little doubt that the concept of terror resounded across the American landscape from the nineteenth century onward.²⁶ From the Black Panthers to the Ku Klux Klan (KKK), from the Workers Party to communist agitators, from Students for a Democratic Society (SDS) to the Weathermen of the Vietnam era, the concept of terror against governing authority was entrenched in the political and social fabric of these organizations (Figure 1.28).

The internal urban violence of the 1960s, triggered and prompted by generations of inequality and injustice, caused law enforcement not only to challenge its historic reactions to public protest but also to see that “enemies” or antagonists of the government may actually be operating from a higher moral plane. The protests could also not be universally condemned because some were plainly justified. Certainly, the entire movement sparked by Dr. Martin Luther King Jr.



Figure 1.28 Public protest against the Vietnam War. (From U.S. Marshal's Service, Pentagon Riot of October 21, 1967.)

1.6 Threats to the Homeland: Revolution, Riot, and Rightful Demonstration

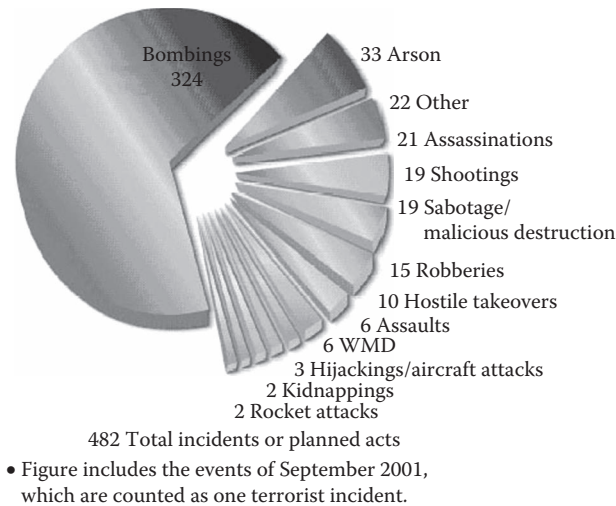


Figure 1.29 Amount of terroristic activities by type of event, 1980–2001.

challenged the status quo of police power and the remediation of injustice. Then too, those operating without moral advantage—groups such as the KKK or the SDS—posed real and meaningful threats against the internal security of the country by their egregious actions. In a sense, both lawful and unlawful protests shaped how the justice model reacted to protest and terror.

For example, during the Nixon era, ordinary citizens were perceived as troublemakers and seditionists for any protest against the policies of the president. Much has been written about the insular and almost paranoid perceptions of Nixon insiders as that government sought to squelch public protest concerning the war in Vietnam.²⁷

Enemies of the state came in many shapes and sizes, some deserving of that name and others not. In the midst of this era, the FBI posted its list of groups that were allegedly anti-American in design.²⁸ During this exceptionally turbulent time, politicians, government officials, and law-enforcement professionals perceived events as a threat to our democratic process.

Internet Exercise: Read about the Weathermen, a subversive antiwar, antigovernment, and anti-capitalist entity active all through the late 1960s–1980s at <http://www.pbs.org/independentlens/weatherunderground/movement.html>.

Throughout the centuries, even up to the present day, we can see that terror has been a tool for those wishing to maintain the status quo as well as those wishing revolution. Hence, it is imperative to remember that the American justice policy has had a historic understanding and relationship with terror throughout most of its history. These acts of terror can be broken down into two essential categories: international and domestic.

Since the early 1960s, the threat of terror has sought to disrupt world economies, overthrow political structures, annihilate religious competitors, and assault value systems considered antagonistic to a perverted worldview. For most of the past 60 years, terror has been on the radar screen. Figure 1.29²⁹ lays out the full scope of terror activities, from bombings to the use of weapons of mass destruction.

1.6.1 Domestic Terrorism: Pre-9/11

Domestic terrorism is considered that which is perpetrated by U.S. nationals and not the product of fringe Islamic extremists or jihadists. Terrorists can equally come from disenfranchised citizens, hate groups, or other extreme wings within the country. There have been some consistent players in terror activities across the American landscape, and surely the KKK fits the bill of



Figure 1.30 Weather Underground leaders John Jacobs (center) and Terry Robbins (right) at the Days of Rage protest march, Chicago, October 1969.

consistency. Political upheaval and radical social change by any means whatsoever appropriately describe the KKK's agenda. For the KKK, terror was central to the mission of the rabid segregationist and promoter of inequality. Historic harassment and lynching have been replaced by slick media and membership campaigns. Regardless of the terrorist's mindset or rationale, history makes clear the motivation behind the tactics.

Domestic terror before the events of 9/11 occurred in a somewhat narrower or localized model, in that the motive for attack was often not on a global scale. Just as the Klansman cares little for what is beyond his or her myopic racism, the student radical, wishing the overthrow of the military complex, cannot see things in global terms. The student radical concludes that a group or a few assembled might wish to publicize their claims in every imaginable way—violence being among its approaches. This was the stuff of the Weathermen—they found banks a legitimate and moral target for destruction in order that a war might end (Figure 1.30).

These operatives see the world in more myopic terms since it is the foundation of their movement that unites them and drives their relationship. In no sense does one justify the actions of the Black Panthers or the Weathermen. This merely demonstrates that a differing worldview exists when compared with the jihadist who ultimately desires the radical reconstruction of the entire planet, and the creation of a caliphate, while imposing a particular religious ideology and zealotry.

1975 TERRORISM FLASHBACK: STATE DEPARTMENT BOMBING

01/29/04

Twenty-nine years ago Thursday, an explosion rocked the headquarters of the U.S. State Department in Washington, D.C. No one was hurt, but the damage was extensive, impacting 20 offices on three separate floors. Hours later, another bomb was found at a military induction center in Oakland, California, and safely detonated. A domestic terrorist group called the Weather Underground claimed responsibility. Remember them?

Who were these extremists? The Weather Underground—originally called the Weathermen, taken from a line in a Bob Dylan song—was a small, violent offshoot of the SDS, created in the turbulent 1960s to promote social change.

1.6 Threats to the Homeland: Revolution, Riot, and Rightful Demonstration

When the SDS collapsed in 1969, the Weather Underground stepped forward, inspired by communist ideologies and embracing violence and crime to protest the Vietnam War, racism, and other left-wing aims. “Our intention is to disrupt the empire ... to incapacitate it, to put pressure on the cracks,” claimed the group’s 1974 manifesto, *Prairie Fire*. By the next year, the group had claimed credit for 25 bombings and would be involved in many more over the next several years.

The Chase. The Federal Bureau of Investigation (FBI) doggedly pursued these terrorists as their attacks mounted. Many members were soon identified, but their small numbers and guerilla tactics helped them hide under assumed identities. In 1978, however, the bureau arrested five members who were plotting to bomb a politician’s office. More were arrested when an accident destroyed the group’s bomb factory in Hoboken, New Jersey. Others were identified after two policemen and a Brinks driver were murdered in a botched armored car robbery in Nanuet, New York.

Success for the FBI/New York Police Department (NYPD) Task Force. Key to disrupting the group for good was the newly created FBI–New York City Police Anti-Terrorist Task Force. It brought together the strengths of both organizations and focused them on these domestic terrorists. The task force and others like it paved the way for today’s Joint Terrorism Task Forces—created by the bureau in each of its field offices to fuse federal, state, and local law enforcement and intelligence resources to combat today’s terrorist threats.

By the mid-1980s, the Weather Underground was essentially history. Still, several of these fugitives were able to successfully hide themselves for decades, emerging only in recent years to answer for their crimes. Once again, it shows that grit and partnerships can and will defeat shadowy, resilient terrorist groups.

One of the more notable domestic terror attacks against the United States was the 1993 attack on New York City’s World Trade Center (Figure 1.31).



Figure 1.31 Investigators going through the rubble following the 1993 bombing of the World Trade Center.

Homeland Security

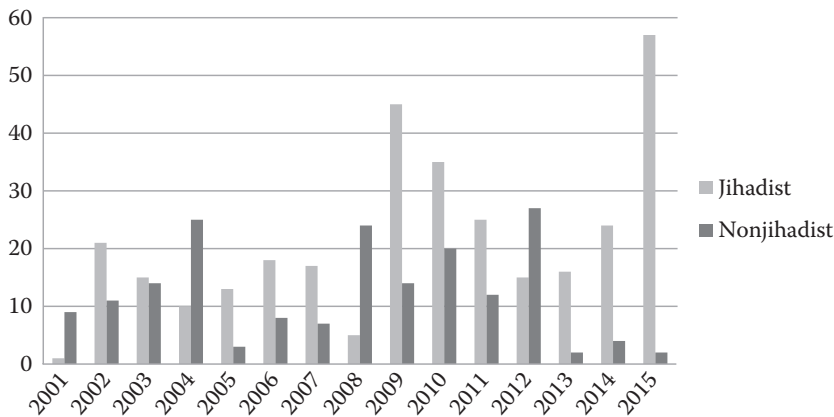


Figure 1.32 Number of extremists indicted or killed from 2001 to 2015. (Courtesy of International Security Data Site at <http://securitydata.newamerica.net/extremists/analysis.html>.)

The boldness of the World Trade Center bombing shocked the Intelligence Community. The sophistication of the plan, the potential for extreme damage and destruction, and the symbolism of the target itself attested to the determination of the terrorist movement long before 9/11.³⁰

Presently, terror finds root in the ideology of religious fanaticism and the jihad. The statistical reality is that jihadi motivation and Islamic extremism are a growing phenomenon and increasing global threat. Figure 1.32 paints an unnerving picture of this undeniable escalation.

Previously, terror was grounded in the ideology of politics and social movements. When the Communist Workers Party clamored for change, its advocacy dealt with the evils of excessive capitalism and the real need for collectivism in the distribution of goods and services. When the Black Panther Party took violent action, it did so with a political revolution in mind and aiming for the whole-scale redress and payback for injustice based on race. Neither of these arguments can justify the violence that these groups offer up, but both groups attest to their dramatically different mindset when compared with that of the extreme and very radical Islamic fundamentalists who flew planes into the Twin Towers or the rationale for the Boston Marathon bombing, whose perpetrators used jihad and Islamic radicalism as a warped rationale for the senseless killing of completely innocent people.³¹ See Figure 1.33.

Terrorism on the domestic front can be driven by diverse motivations. Race hatred, white supremacy, protests against governmental policy, and an inordinate desire to subvert and undermine the nature of the democratic state are just a few of the rationales employed. Timothy McVeigh's bombing of the federal building in Oklahoma City manifests the disproportionate dislike and distrust of government in any sense and the extreme alienation and isolation that certain terrorists seem to experience in light of the democratic process. That government may or may not be too intrusive cannot provide enough justification for murder, but the level of distrust and flat-out antagonism toward government is a growing phenomenon in select quarters.

Ted Kaczynski (aka the Unabomber) also reflects this loner, antigovernment tradition of the terrorist. In his "manifesto," Kaczynski railed against most aspects of modern life, industrialization, the loss of freedom, and the invasiveness of government. Kaczynski's arrest, one of the FBI's most successful apprehensions, was celebrated and recollected in 2008.³²

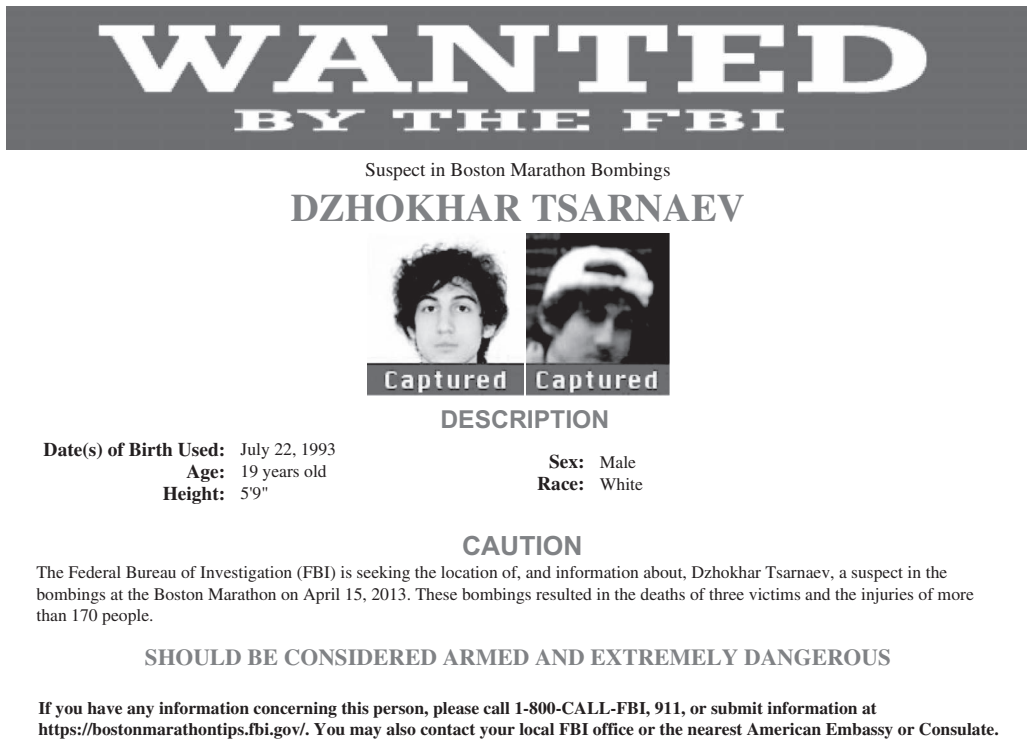


Figure 1.33 Dzhokhar Tsarnaev's FBI "Wanted" poster. (<https://www.fbi.gov/wanted/alert/dzhokhar-tsarnaev>.)

FBI 100: THE UNABOMBER

04/24/08

Part 4 of Our History Series Commemorating the FBI's 100th Anniversary in 2008

How do you catch a twisted genius who aspires to be the perfect, anonymous killer—who builds untraceable bombs and delivers them to random targets, who leaves false clues to throw off authorities, who lives like a recluse in the mountains of Montana and tells no one of his secret crimes?

That was the challenge facing the FBI and its investigative partners, who spent nearly two decades hunting down this ultimate lone wolf bomber.

The man that the world would eventually know as Theodore Kaczynski came to our attention in 1978 with the explosion of his first, primitive homemade bomb at a Chicago university. Over the next 17 years, he mailed or hand delivered a series of increasingly sophisticated bombs that killed three Americans and injured 24 more. Along the way, he sowed fear and panic, even threatening to blow up airliners in flight.

In 1979, an FBI-led task force that included the ATF and U.S. Postal Inspection Service was formed to investigate the "UNABOM" case, code-named for the University and Airline Bombing targets involved. The task force would grow to more than 150 full-time investigators, analysts, and others. In search of clues, the team made every possible forensic examination of recovered bomb components and studied the lives of victims in

minute detail. These efforts proved of little use in identifying the bomber, who took pains to leave no forensic evidence, building his bombs essentially from “scrap” materials available almost anywhere. And the victims, investigators later learned, were chosen randomly from library research.

We felt confident that the Unabomber had been raised in Chicago and later lived in the Salt Lake City and San Francisco areas. This turned out to be true. His occupation proved more elusive, with theories ranging from aircraft mechanic to scientist. Even the gender was not certain: although investigators believed the bomber was most likely male, they also investigated several female suspects.

The big break in the case came in 1995. The Unabomber sent us a 35,000-word essay claiming to explain his motives and views of the ills of modern society. After much debate about the wisdom of “giving in to terrorists,” FBI Director Louis Freeh and Attorney General Janet Reno approved the task force’s recommendation to publish the essay in hopes that a reader could identify the author.

After the manifesto appeared in *The Washington Post* and *The New York Times*, thousands of people suggested possible suspects. One stood out: David Kaczynski described his troubled brother Ted, who had grown up in Chicago, taught at the University of California at Berkeley (where two of the bombs had been placed), then lived for a time in Salt Lake City before settling permanently into the primitive 10’×14’ cabin that the brothers had constructed near Lincoln, Montana (Figure 1.34).

Most importantly, David provided letters and documents written by his brother. Our linguistic analysis determined that the author of those papers and the manifesto were almost certainly the same. When combined with facts gleaned from the bombings and Kaczynski’s life, that analysis provided the basis for a search warrant.

On April 3, 1996—a dozen years ago this month—investigators arrested Kaczynski and combed his cabin (Figure 1.35). There, they found a wealth of bomb components; 40,000 handwritten journal pages that included bomb-making experiments and descriptions of Unabomber crimes; and one live bomb, ready for mailing.

Kaczynski’s reign of terror was over. His new home, following his guilty plea in January 1998: an isolated cell in a “Supermax” prison in Colorado.³³



Figure 1.34 Ted Kaczynski’s cabin in the mountains of Montana.

1.6 Threats to the Homeland: Revolution, Riot, and Rightful Demonstration



Figure 1.35 Ted Kaczynski, aka the Unabomber.

The array of terror groups include those advocating radical change involving racist ideologies, religious bigotry and hatred, economic overthrow of existing governmental structures, and ideologies relating to the environment and animal rights. These groups are capable of inflicting extraordinary damage on the country, and they must remain on the radar screen of those entrusted with the security of the United States and its citizens.

1.6.2 International Terrorism: Pre-9/11

Just as in the United States, the international community had experienced a series of attacks from various constituencies. One of the more notable overseas terror attacks against the United States was at the Marine base in Beirut, Lebanon, in 1983, where 241 servicemen lost their lives (Figure 1.36).

The attack in Lebanon, in a secure military environment, made plain the tenacity of the terrorist and the willingness of this enemy to tackle any target, no matter how formidable. This attack sent a vivid reminder to the government and military that terrorism was a growing and very dangerous reality.

During the 1980s, organized terrorist groups that we have come to know only too well—al-Qaeda, Hamas, and Hezbollah—gained foundational and organizational support from many



Figure 1.36 The aftermath of the attack on the Marine base in Lebanon. (From Department of Defense.)



Figure 1.37 The USS *Cole* suffered the loss of 17 crewmen, representing the first attack against a naval vessel of the United States in nearly 25 years. (From Department of Defense by Sgt. Don L. Maes, U.S. Marine Corps.)

quarters in both a political and an economic sense. By the 1990s, Osama bin Laden had developed a network of terrorists eager to carry out attacks.

In Yemen and Somalia, Bin Laden funded, planned, and orchestrated acts that killed and injured a number of U.S. soldiers. Eighteen Special Forces members were attacked and killed in Somalia in 1993. In 1996, Bin Laden set out to attack the Khobar Towers in Saudi Arabia, where 19 American airmen died. In August 1998, Bin Laden and al-Qaeda bombed the embassies of Kenya and Tanzania, which resulted in the death and injury of thousands of innocents. Al-Qaeda and Bin Laden were getting even bolder as time progressed, carrying out a direct attack on a U.S. warship—the USS *Cole*—in Yemen in 2000 (Figure 1.37). Using a small boat as a suicide projectile, al-Qaeda operatives displayed unparalleled methods in carrying out their attack.

None of these events occurred in a vacuum but rather as a progressive series of events that eventually culminated in the single largest attack by a foreign enemy on American soil. Each attack displayed an evolving aggressiveness toward America, each attack employed a variety of tactics to keep the defenders off guard, and each attack manifested an increasing fanaticism in the Islamic extremist world. Succinctly, 9/11 did not occur out of the blue. Terror has a progressive history. As the world memorializes the twentieth anniversary of 9/11, it is imperative that justice professionals and citizens alike remember the historical underpinnings of terror, the threads of continuity in using hate and malice to effect and impact change and the full acceptance that every form of terror is not a fixed or absolute state of affairs but instead, a fluid and constantly evolving ideology coupled with emerging methods and protocols to inflict human misery. Terror is not static or fixed by design but rather a continuously evolving form of evil.³⁴

1.7 Conclusion

The concepts of terror and the terrorist have a long and perpetual history on both the domestic and international fronts. Terrorists have always been with us in one way or another. In this short survey, the reader learns the events and conditions that led up to our present definition of terror. The chapter commences with a look at how war, military tactics and strategy, and aligned governmental policy frequently employ terror tactics. Then, the reader is exposed to how the Cold

War mentality shaped our perceptions about terror and subterfuge and weighed and evaluated how government policy can be influenced by events and conditions that can make once repressive regimes into more open societies. The chapter then shifts to terrorism as it existed before 9/11. The American experience has long had vestiges of terror in its social fabric. Special attention is given to the KKK, the Weathermen, the Black Panthers, and the SDS, as well as newly developing and ever-evolving groups espousing hatred. Terrorism, pre-9/11, was rooted in differing motivations ranging from racism to a desire for change and revolution.

By the 1990s, the face of terrorism adopted a virulent form of antigovernment sentiment, evidenced by the likes of Ted Kaczynski and Timothy McVeigh. Each had more than an ax to grind and sought to destroy what he perceived as a corrupt culture and government. In addition, pre-9/11, there was the rise of Islamic jihadists who carried out several international attacks, most coordinated by Osama bin Laden and others who followed him.

Hijackings, terror in the skies, embassy bombings, the kidnapping of American personnel, and attacks on naval targets became commonplace events of terror. All of this culminated in the catastrophe of 9/11—events and circumstances that are still overwhelmingly shocking and tragic. More particularly, the chapter looks at the attacks on the USS *Cole* and the Marine post in Lebanon.

As a direct result of 9/11, the missions of multiple U.S. agencies would undergo exceptional reorientation. In addition, these same agencies would become part of the newly constructed agency—the Department of Homeland Security.

Keywords

Al-Qaeda; Allies; Berlin Wall; Black Panthers; Cold War; Communism; Communist Workers Party; Cuban Missile Crisis; Domestic Terrorism; Dzhokhar Tsarnaev; Final Solution; Hamas; Harry S. Truman; Hezbollah; Homeland Security; Human Rights; Imperialism; Iron Curtain; ISIS/ISIL; Islamic Fundamentalism; Jihad; Joseph Stalin; Korean War; Ku Klux Klan; Mikhail Gorbachev; Nikita Khrushchev; Nuclear Proliferation; Osama bin Laden; Potsdam Convention; Religious Fanaticism; Richard Nixon; Robert Bowers; Ronald Reagan; Saddam Hussein; Sino-Soviet; Soviet Communist Party; Students for a Democratic Society; Ted Kaczynski; Terror; Terrorist; Third Reich; Timothy McVeigh; Tree of Life Synagogue; Truman Doctrine; Vietnam War; Weathermen; Winston Churchill

Discussion Questions

1. When one evaluates the past 50 years of terrorist activities, what threats or trends can be discovered? Is there a commonality of purpose or type?
2. Why do terrorists so often choose embassies as targets?
3. In what way are Timothy McVeigh and Osama bin Laden the same?
4. Compare and contrast domestic and international terrorism. Point out the differences.
5. What are the motivations of terrorist groups in the pre-9/11 world compared with the post-9/11 world?
6. How can war be an instrument of terror?
7. Is it fair to argue that the United States engaged in terror during any of its war campaigns?
8. What does the Cold War teach us about the transient nature of the terror threat?

Homeland Security

9. Was the Cold War threat different from the USS *Cole* threat?
10. Is the aim of the Unabomber similar to that of Osama bin Laden?
11. Discuss how religious ideology provides a justification, however irrational, for acts of terror. How has religion been used nationally and internationally as a basis for terror?

Practical Exercises

1. Find out whether or not a revolutionary group such as the Aryan Brotherhood or the KKK still operates in your area.
2. Are you aware of any paramilitary organizations that train in your region?
3. What type of terror prevention programs does your area have to root out domestic terrorists?
4. Contact your local police chief. Ask whether or not he or she sees any real threats from local groups that might engage in terrorist activity.
5. Visit the Truman or Reagan Library online for a virtual tour.
6. Determine whether your community engages in religious or ecumenical dialogue, and public engagement on the nature of terrorism. Are all religious sects involved or are some silent?
7. Find out about the rising tide of terrorist activities against religious entities. Visit the FBI's web portal at: https://www.fbi.gov/file-repository/developing_eops_for_houses_of_worship_final.pdf/view

Notes

- 1 See: Rand Corporation, "Domestic Terrorism," <https://www.rand.org/topics/domestic-terrorism.html> (accessed August 8, 2020).
- 2 See: "Dismantling China's Muslim gulag in Xinjiang is not Enough," *The Economist*, January 9, 2020, <https://www.economist.com/leaders/2020/01/09/dismantling-chinas-muslim-gulag-in-xinjiang-is-not-enough> (accessed August 8, 2020).
- 3 J. Sudworth, "China's Hidden Camps," *BBC News*, October 24, 2018, <https://www.bbc.co.uk/news/resources/181024-china-hidden-camps> (accessed August 8, 2020).
- 4 North American Treaty Organization, W. S. Churchill, *The Sinews of Peace*, http://www.nato.int/docu/speech/1946/S460305a_e.htm (accessed August 8, 2020).
- 5 T. Lister, *ISIS: The first terror group to build an Islamic state?* CNN.com, <http://www.cnn.com/2014/06/12/world/meast/who-is-the-isis/index.html> (accessed August 8, 2020); *Business Insider*, maps show the progression of ISIS control in Iraq and Syria, <http://www.businessinsider.com/these-maps-show-the-progression-of-isis-control-in-iraq-and-syria-2015-8> (accessed August 8, 2020).
- 6 See: J. Poor, "Blackburn: China Part of the 'New Axis of Evil,' along with North Korea, Iran And Russia," *American Priority*, April 12, 2020, <https://americanpriority.com/news/blackburn-china-part-of-the-new-axis-of-evil-along-with-north-korea-iran-and-russia/> (accessed August 8, 2020); For a full analysis of how North Korea has become part of this new "axis," see ACE Threats Integration, Threat Tactics Report: North Korea versus the United States, US Army TRADOC G-2 (March 2018), <https://info.publicintelligence.net/USArmy-NKvsUSTactics.pdf> (accessed August 8, 2020).

- 7 The Ronald Reagan Presidential Foundation & Library, President R. L. Reagan, *Remarks on East-West Relations at the Brandenburg Gate in West Berlin*, June 12, 1987, <https://www.reaganfoundation.org/ronald-reagan/reagan-quotes-speeches/remarks-on-east-west-relations-at-the-brandenburg-gate-in-west-berlin/> (accessed August 8, 2020).
- 8 E. D. Johnson, Putin and Putinism, *The Slavonic and East European Review*, 89(3) (2011): 788–790.
- 9 M. R. Gordon, U.S. Begins Military Talks with Russia on Syria, *The New York Times Online*, September 18, 2015, <https://www.nytimes.com/2015/09/19/world/europe/us-to-begin-military-talks-with-russia-on-syria.html?searchResultPosition=1> (accessed August 8, 2020); A. Tilghman, U.S., Russia Resume Military Relations to “deconflict” in Syria, *Military Times*, September 18, 2015, <http://www.militarytimes.com/story/military/pentagon/2015/09/18/russia-mil-to-mil/72395558/> (accessed August 8, 2020).
- 10 See: National Security Archive, “1979 Iran Hostage Crisis Recalled,” M. Byrne, ed. (November 4, 2019), <https://nsarchive.gwu.edu/briefing-book/iran/2019-11-04/1979-iran-hostage-crisis-recalled> (accessed August 8, 2020).
- 11 See: “Intensified Sanctions on Iran,” Press Statement by M. R. Pompeo, Secretary of State, January 10, 2020, <https://www.state.gov/intensified-sanctions-on-iran/> (accessed August 8, 2020).
- 12 DIA, “Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance,” (November 2019) (accessed November 23, 2020).
- 13 See: DHS Intelligence Enterprise (DHS IE) Counterterrorism Mission Center (CTMC), “Worldwide Terrorist Operations Linked to Lebanese Hizballah or Iran: Observed Behaviors and Key Indicators of Suspicious Activities,” (July 15, 2019), <https://info.publicintelligence.net/DHS-HizballahIranTerroristOperations.pdf> (accessed August 8, 2020).
- 14 Ibid.
- 15 See: Patrick Wintour, “Persecution of Christians ‘coming close to genocide’ in Middle East – Report,” *The Guardian*, May 2, 2019, <https://www.theguardian.com/world/2019/may/02/persecution-driving-christians-out-of-middle-east-report> (accessed August 8, 2020); see also: E. M. Brown, Persecution of Christians in Muslim-Majority Countries, *Journal of Ecumenical Studies*, (51)2 (2016): 198–209, <https://muse.jhu.edu/article/627331/pdf> (accessed August 8, 2020).
- 16 See: J. T. Caruso, Testimony before the Subcommittee on International Operations and Terrorism, Committee on Foreign Relations, United States Senate, Washington, D.C., December 8, 2001, <https://archives.fbi.gov/archives/news/testimony/al-qaeda-international> (accessed August 8, 2020).
- 17 US Government Accountability Office, “Countering Isis and Its Effects: Key Issues for Oversight” 6, Figure 2 (July 2017), <https://www.gao.gov/assets/690/685908.pdf> (accessed August 8, 2020).
- 18 Mapping Militant Organizations. “The Islamic State.” Stanford University. Last modified September 2019, <http://web.stanford.edu/group/mappingmilitants/cgi-bin/maps/view/islamic-state> (accessed August 8, 2020).
- 19 J. Davenport, “Syria Civil War Key Points,” <https://faculty.fordham.edu/davenport/Syria/Syria-History.html> (accessed August 8, 2020).
- 20 See: US Department of Defense, “Nuclear Posture Review,” (January 2018), <https://info.publicintelligence.net/DoD-NuclearPostureReviewDraft-2018.pdf> (accessed August 8, 2020).
- 21 Central Intelligence Agency (CIA), The World Factbook, <https://www.cia.gov/library/publications/the-world-factbook/geos/kn.html> (accessed August 8, 2020).
- 22 J. H. Pak, “The Education of Kim Jong-Un,” (February 2018), <https://www.brookings.edu/essay/the-education-of-kim-jong-un/> (accessed August 8, 2020).
- 23 See: “South v North Korea: How do the two countries compare? Visualised,” *The Guardian*, <https://www.theguardian.com/world/datablog/2013/apr/08/south-korea-v-north-korea-compared>, Information obtained from the CIA World Fact Book, Reporters without Borders, World Bank, Foreign Policy HSS military Balance 2012 (accessed August 8, 2020).
- 24 For Congressional Hearings gauging the extent of these sales, see: Joint Hearing before the Subcommittee on Terrorism, Nonproliferation, and Trade and the Subcommittee on Asia and the Pacific and the Subcommittee on the Middle East and North Africa of the Committee on Foreign Affairs, House of Representatives, 114th Congress, 1st Session, July 28, 2015, <https://www.govinfo.gov/content/pkg/CHRG-114hhrg95694/html/CHRG-114hhrg95694.htm> (accessed August 8, 2020).

Homeland Security

- 25 See: U.S. Army, “Threat Tactics Report: North Korea,” December 29, 2017, <https://publicintelligence.net/usarmy-north-korea-tactics/> (accessed August 8, 2020); See also a comparison of armies and weapons at: ACE Threats Integration, Threat Tactics Report: North Korea versus the United States, US Army TRADOC G-2 (March 2018), <https://info.publicintelligence.net/USArmy-NKvsUSTactics.pdf> (accessed August 8, 2020).
- 26 For an interesting analysis of the Ku Klux Klan as it rationalized its hatred with the fervor of false patriotism, see P. D. Brister, Patriotic enemies of the state: A cross comparison of the Christian Patriot Movement and the 1920’s Ku Klux Klan, *The Homeland Security Review*, 4 (2010): 173.
- 27 R. Perlstein, *Nixonland: America’s Second Civil War and the Divisive Legacy of Richard Nixon, 1965–1972* (New York: Simon & Schuster, 2008).
- 28 G. R. Stone, *Review of Spying on Americans: Political Surveillance from Hoover to the Huston Plan*, by Athan Theoharis, *Reviews in American History*, 8(1) (March 1980): 134–138. For a full analysis of how the Weathermen worked, see Federal Bureau of Investigation, Weathermen Underground Summary, dated 8/20/76, [https://vault.fbi.gov/Weather%20Underground%20\(Weathermen\)](https://vault.fbi.gov/Weather%20Underground%20(Weathermen)) (accessed August 8, 2020).
- 29 Federal Bureau of Investigation, *Terrorism 2000–2001*, Publication 0308 (Washington, DC: U.S. Government Printing Office, 2004), 16.
- 30 U.S. Fire Administration, *The World Trade Center Bombing: Report and Analysis*, W. Manning, ed. (Washington, DC: U.S. Government Printing Office, 1993), 15. For a comparison of the 1993 emergency reaction with that of 2001, see R. F. Fahy and G. Proulx, *A Comparison of the 1993 and 2001 Evacuation of the World Trade Center, Proceedings of the 2002 Fire Risk & Hazard Assessment Research Application Symposium* (Fire Protection Research Foundation, Quincy, MA), 111–117. For a close look at how the World Trade Center bombings caused extraordinary upheaval from a social, behavioral, and health perspective, see R. E. Adams, J. A. Boscarino, and S. Galea, Social and psychological resources and health outcomes after the World Trade Center disaster, *Social Science & Medicine*, 62 (2006): 176–188, <http://www.sciencedirect.com/science/article/pii/S027795360500239X>.
- 31 Reuters Boston Marathon Bombing archive, www.reuters.com.
- 32 Federal Bureau of Investigation, Headline archives, The Unabomber, https://www.fbi.gov/news/stories/2008/april/unabomber_042408 (accessed August 8, 2020).
- 33 Ibid.
- 34 In present times, no better proof of this argument can be found than how the role of ISIS has played out over the last decade. To dominance to a crushed, shrinking state, ISIS can never be termed static. See: US Government Accountability Office, “Countering Isis and Its Effects: Key Issues for Oversight” (July 2017), <https://www.gao.gov/assets/690/685908.pdf> (accessed August 8, 2020).

2

Terror, Threat, and Disaster Post 9/11: A New Paradigm of Homeland Security

OBJECTIVES

1. To analyze the events of 9/11 and understand the effect they had on the American population's psyche in relation to domestic security
2. To identify and assess post-9/11 threats with an emphasis on lessons learned
3. To appraise the effectiveness of the immediate response by government agencies to the events of 9/11
4. To describe the shortcomings of the lack of information exchange between various government agencies prior to 9/11 and analyze the influence the lack of communication had on the day's events
5. To outline the new strategies and tactics that the safety community developed for the mitigation and prevention of terrorism immediately following 9/11
6. To describe the initial formation of the Department of Homeland Security (DHS), its structure, and policy approach, mission, and goals
7. To explain the structural changes that have taken place in DHS since its inception
8. To summarize DHS's hierarchy, major players, and various advisory committees
9. To list the various directorates and offices of DHS and discuss their mission and responsibilities
10. To evaluate various DHS policies and practices over a 20-year cycle

2.1 Introduction

To say the world changed on September 11, 2001, is an extraordinary understatement. As the air assault on the Twin Towers and the Pentagon unfolded, both government agencies and the general populace watched in stunned silence. Even today, it is difficult to fathom the full and sweeping implications of such an attack. Dual plane attacks on the Twin Towers of the World Trade Center are almost impossible to fathom. Yet, this is exactly what occurred. Radical Islamic extremists perpetrated the deadliest attack carried out on U.S. soil (Figure 2.1).¹

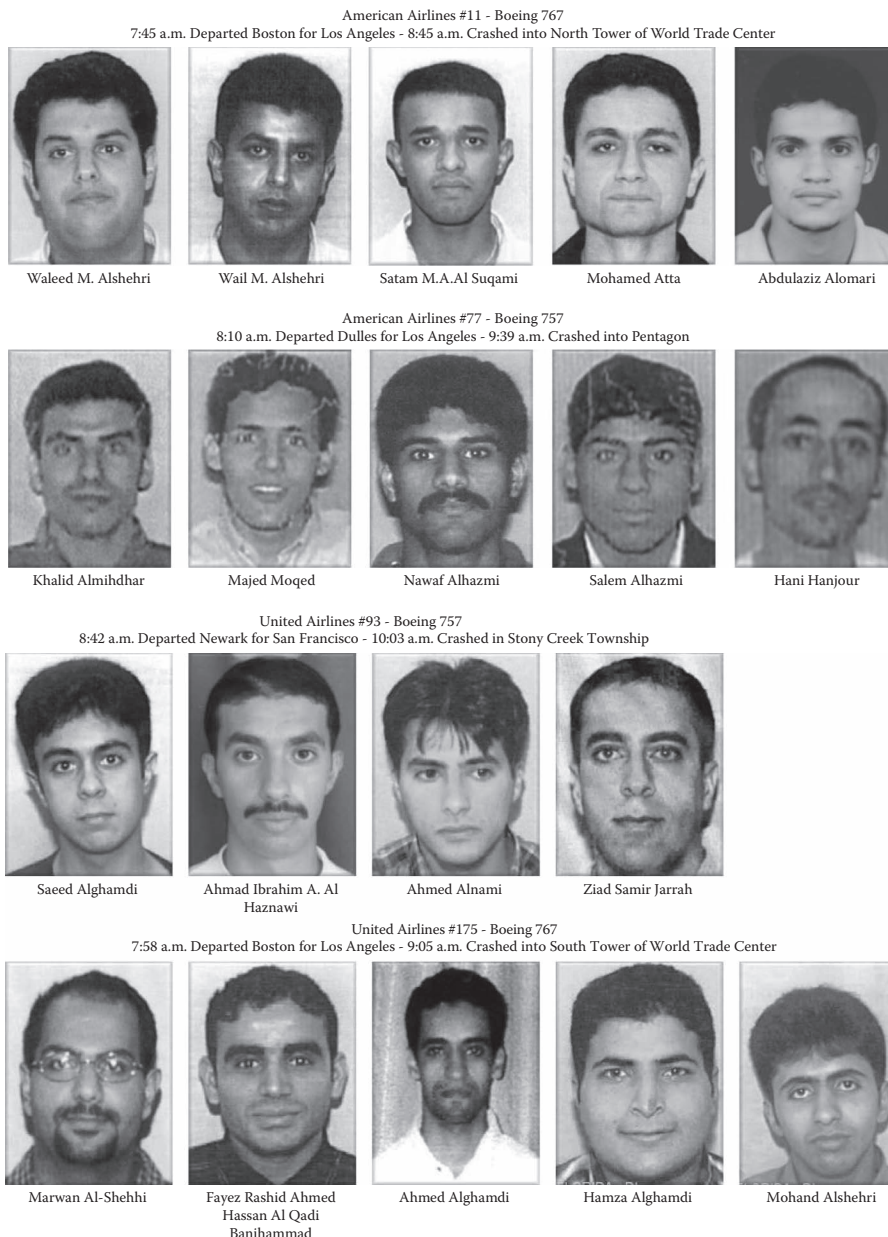


Figure 2.1 Terrorists aboard the four hijacked flights on September 11, 2001. (Courtesy of the Federal Bureau of Investigation, Washington, D.C.)

2.1 Introduction

The damage to New York's financial district was catastrophic. Not only was the loss of life at staggering proportions, but the economic impact on the New York metropolitan area and the country was significant (Figures 2.2–2.4).

Notions of security would be forever challenged and altered. Ideas of safety within America's borders would now be doubted. Indeed, the last 5 years have been witness to an intense debate on what borders really mean and even, to the complete consternation of experienced law enforcement sectors responsible for the border, whether borders should be closed or opened. The more progressive politicians are claiming ICE enforcement mimics Nazi-like tactics and that the agency

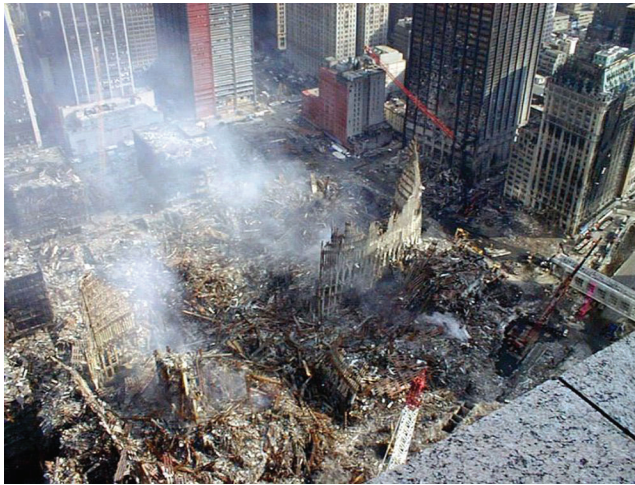


Figure 2.2 Twin Towers rubble after the collapse. (www.whitehouse.gov.)



Figure 2.3 National Guard members at the Twin Towers disaster site. (www.fema.gov.)



Figure 2.4 The Pentagon after the fires were extinguished. (www.fema.gov.)

should be completely abolished. U.S. Congresswoman Alexandria Ocasio-Cortez has described the entire border processing and barriers to free and unbridled entry as “systematic cruelty.”² Congresswoman Ilhan Omar equates border detention centers with “concentration camps” and at the same time calls for the complete elimination of ICE and “other rogue agencies.”³ At present, the country suffers under a split, divisive vision on the question of border control—some urging a forceful and protective attitude toward our sovereignty,⁴ while others see border restriction as some xenophobic reaction to cultural differences. Ultimately how a country can sustain itself, protect itself, and preserve its fundamental identity and human and physical assets without any border remains nothing more than a well-intentioned but implausible dream.⁵ How this nation moved to fairly consistent unanimity on border matters to such widely varying opinions on policy can only be described as an extraordinary shift in selected public sentiments.

Internet Exercise: See the actual construction of the Border Wall in El Centro, TX at: <https://www.cbp.gov/border-security/along-us-borders/border-wall-system>

2.2 Genesis of DHS

Confidence in our ability to withstand or detect attacks was severely undermined by the events of 9/11. The attacks on American soil were sweeping in scope and left the public safety and law enforcement communities stunned. How could planes be hijacked and crashed into the financial district of one of the largest American cities? How could the walls of the Pentagon be breached? How could a plane crash in rural Pennsylvania represent a thwarted bid to attack the White House (Figure 2.5)?

The complexity of the undertaking manifests a well-prepared and very determined enemy. The timeline of the attacks says much about the complexity of these events (see Figure 2.6).⁶

It is impossible to measure the complete impact that these events had upon the American psyche, the former invincibility of our home soil, and the pronounced re-examination of our entire approach to law enforcement and the overall security of a nation (Figure 2.7).⁷

As one illustration, the Federal Bureau of Investigation (FBI), while historically concerned about the potential random acts of terrorists, had to shift into a more intense scrutiny of the terrorist impact on our way of life. The National Commission on 9/11 was attuned to this strategic shift when it wrote:

Collection of useful intelligence from human sources was limited. By the mid-1990s senior FBI managers became concerned that the bureau’s statistically driven performance system had resulted in a roster of mediocre sources. The FBI did not have a formal mechanism for validating source



Figure 2.5 United Flight 93 in Shanksville, Pennsylvania. (www.fema.gov)

8 a.m. -- American Airlines Flight 11, Boeing 767 with 92 people on board, takes off from Boston's Logan International Airport for Los Angeles.

8:14 a.m. -- United Air Lines Flight 175, Boeing 767 with 65 people on board, takes off from Boston's Logan airport for Los Angeles.

8:21 a.m. -- American Airlines Flight 77, Boeing 757 with 64 people on board, takes off from Washington Dulles International Airport for Los Angeles.

8:40 a.m. -- Federal Aviation Administration notifies North American Aerospace Defense Command's Northeast Air Defense Sector about suspected hijacking of American Flight 11.

8:41 a.m. -- United Air Lines Flight 93, Boeing 757 with 44 people on board, takes off from Newark International Airport for San Francisco.

8:43 a.m. -- FAA notifies NORAD's Northeast Air Defense Sector about suspected hijacking of United Flight 175.

8:46 a.m. -- American Flight 11 crashes into north tower of World Trade Center.

9:03 a.m. -- United Flight 175 crashes into south tower of World Trade Center.

9:08 a.m. -- FAA bans all takeoffs nationwide for flights going to or through New York airspace.

9:17 a.m. -- FAA closes down all New York City-area airports.

9:21 a.m. -- All bridges and tunnels into Manhattan closed.

9:24 a.m. -- FAA notifies NORAD's Northeast Air Defense Sector about suspected hijacking of American Flight 77.

9:26 a.m. -- FAA bans takeoffs of all civilian aircraft.

9:31 a.m. -- In Sarasota, Fla., President Bush calls crashes an "apparent terrorist attack on our country."

Figure 2.6 Chronology of the key events of September 11, 2001 (all times Eastern).

(Continued)

Homeland Security

9:40 a.m. (approx.) -- American Flight 77 crashes into Pentagon.

9:45 a.m. -- FAA orders all aircraft to land at nearest airport as soon as practical. More than 4,500 aircraft in air at the time. This is the first time in U.S. history that nationwide air traffic is suspended.

9:48 a.m. -- U.S. Capitol and White House's West Wing evacuated.

9:57 a.m.-- President Bush leaves Florida.

9:59 a.m. -- South tower of World Trade Center collapses.

10:07 a.m. (approx.) -- United Flight 93 crashes in a field in Shanksville, Pa., southeast of Pittsburgh.

10:28 a.m. -- North tower of World Trade Center collapses.

10:50 a.m. -- New York's primary elections, scheduled for Sept. 11, are postponed.

10:56 a.m. -- Palestinian leader Yasser Arafat speaks in Gaza: "First of all, I am offering my condolences, the condolences of the Palestinian people, to their American President, President Bush, to his government, to the American people, for this terrible time. We are completely shocked, completely shocked. Unbelievable."

11 a.m. -- New York City Mayor Rudolph W. Giuliani orders the evacuation of lower Manhattan south of Canal Street.

11:04 a.m.-- The United Nations is fully evacuated.

12:04 p.m. -- Los Angeles International Airport, the destination of three of the hijacked airplanes, is closed and evacuated.

12:15 p.m. -- San Francisco International Airport, the destination of United Airlines Flight 93, which crashed in Pennsylvania, is closed and evacuated.

12:30 p.m. -- The FAA says 50 flights are in U.S. airspace, but none are reporting any problems.

1:04 p.m. -- From Barksdale Air Force base in Louisiana, Bush announces U.S. military on high-alert worldwide: "Make no mistake: The United States will hunt down and punish those responsible for these cowardly acts."

1:37 p.m. -- Bush leaves Barksdale for Offutt Air Force Base, near Omaha, Neb.

2:51 p.m. -- Navy dispatches missile destroyers to New York, Washington.

3:07 p.m. -- Bush arrives at U.S. Strategic Command at Offutt Air Force Base in Neb.

4:36 p.m. -- Bush leaves Offutt Air Force Base aboard Air Force One to return to Washington.

5:25 p.m. -- The empty, 47-story Seven World Trade Center collapses.

7 p.m. -- Bush arrives at the White House.

8:30 p.m. -- Bush addresses nation and vows to "find those responsible and bring them to justice."

Figure 2.6 (*CONTINUED*) Chronology of the key events of September 11, 2001 (all times Eastern).



Figure 2.7 Workers in the rubble of the Twin Towers. (www.fema.gov.)

reporting, nor did it have a system for adequately tracking and sharing such reporting, either internally or externally. The “wall” between criminal and intelligence investigations apparently caused agents to be less aggressive than they might otherwise have been in pursuing Foreign Intelligence Surveillance Act (FISA) surveillance powers in counterterrorism investigations. Moreover, the FISA approval process involved multiple levels of review, which also discouraged agents from using such surveillance. Many agents also told us that the process for getting FISA packages approved at FBI headquarters and the Department of Justice was incredibly lengthy and inefficient. Several FBI agents added that, prior to 9/11, FISA-derived intelligence information was not fully exploited but was collected primarily to justify continuing the surveillance. The FBI did not dedicate sufficient resources to the surveillance or translation needs of counterterrorism agents. The FBI’s surveillance personnel were more focused on counterintelligence and drug cases. In fact, many field offices did not have surveillance squads prior to 9/11. Similarly, the FBI did not have enough translators proficient in Arabic and other languages useful in counterterrorism investigations, resulting in a significant backlog of untranslated FISA intercepts by early 2001. FBI agents received very little formalized training in the counterterrorism discipline. Only 3 days of the 16-week new agent’s course were devoted to national security matters, including counterterrorism and counterintelligence, and most subsequent counterterrorism training was received on an *ad hoc* basis or “on the job.” Additionally, the career path for agents necessitated rotations between headquarters and the field in a variety of work areas, making it difficult for agents to develop expertise in any particular area, especially counterterrorism and counterintelligence. We were told that very few FBI field managers had any counterterrorism experience, and thus either were not focused on the issue or did not have the expertise to run an effective program.⁸

Aside from a lack of coordination and interagency cooperation, the events of 9/11 make plain that an actual wall did exist between the varied agencies of government. The Central Intelligence Agency (CIA) did not share with the FBI, state and local police did not communicate readily, and jurisdictional and turf issues often influenced policy making in the pre-9/11 world. “The absence of coordination and collaboration in the area of information and intelligence sharing contributed to the surprise of the attack.”⁹ After 9/11, it was blatantly obvious that walls had to be torn down and new infrastructures and agencies created based on a cooperative mentality. But this tendency not to collaborate and share appears a problem that continues even 20 years after the tragic events of 9/11. Case after case, especially when it comes to domestic terrorism, active shooters and crazed criminals illustrate how agencies keep information to itself instead of sharing. So often, after the fact, one hears that a suspect was under FBI surveillance, or on the radar screen due to a past criminal history or connected to foreign support groups advancing terrorism—this sort of knowledge commonly known by intelligence agencies. Too often, the FBI

Rubio: FBI Utterly Failed Victims of Florida Shooting

FEB 16 2018

Washington, D.C. – U.S. Senator Marco Rubio (R-FL) released the following statement today after the Federal Bureau of Investigation (FBI) failed to follow protocols after receiving tips regarding the Parkland, Florida shooter:

“It is inexcusable that the FBI failed to follow protocols and inform the Miami Field Office that people close to the Parkland, FL shooter warned the Bureau over a month ago of his desire to kill, his mental state, and erratic behavior. The fact that the FBI is investigating this failure is not enough. Both the House and Senate need to immediately initiate their own investigations into the FBI’s protocols for ensuring tips from the public about potential killers are followed through. Lawmakers and law enforcement personnel constantly remind the public that ‘if you see something, say something.’ In this tragic case, people close to the shooter said something, and our system utterly failed the families of seventeen innocent souls.”

Figure 2.8 February 16, 2018, Senator Marco Rubio’s statement on the Parkland shooting.

still does not know what the CIA should be disclosing and vice versa, or local law enforcement has no knowledge about a particular individual with propensities for violence and terroristic acts. The cases of failed collaboration are far too common. The Parkland High School Shooting case, where 17 students were slaughtered by Nikolas Kruz, signifies an FBI catastrophic disclosure error when it failed to advise the school or local law enforcement of a real and impending threat.¹⁰

Internet Exercise: For a troubling PowerPoint presentation, produced by the Florida Department of Law Enforcement on how many signs regarding Kruz’s propensity to commit terror at this level, see: <http://www.fdle.state.fl.us/MSDHS/Meetings/November-Meeting-Documents/Nov-13-145pm-Cruz-Behavior-Chris-Lyons.aspx>

Florida Senator Marco Rubio was unequivocal in his condemnation of this failure when he issued the press release in 2018 (Figure 2.8).¹¹

The historic resistance to shared, collaborative information remains a constant challenge of governmental agencies so large and so byzantine that it is difficult to change the culture of ownership these entities have long preserved. While there continue to be mistakes, especially in failing to warn and give advice to state and local officials, there has been improvement. And the sharing mentality goes further than inter-government agency relations and now includes private business entities. In the 2015 San Bernardino shooting by the husband and wife terrorist team of Rizwan Farook and Tashfeen Malik, who were killed in the ensuing chase and gun-battle, the FBI could not gain access to the terrorist’s cell phones—both of which were Apple encrypted—and which Apple refused to unlock. See Figure 2.9.

Due to privacy concerns, Apple claimed it could not unlock the phones for the FBI to gather intelligence. This is not a new problem for the FBI which apparently has been locked out of more than 8,000 Apple phones.¹²

In general, law enforcement and emergency management authorities must see the world in a post-9/11 prism, fully recognizing that what once was effective in cases of mass terror, is no longer viable. “There are significant changes not only in the daily lives of the American people but also in the function of the country’s emergency management system.”¹³ In matters of command, communication, deployment, planning, and dispatch, traditional agencies were challenged in ways never before envisioned. Nothing in the status quo could have operationally prepared these professionals for a post-9/11 world. And in a sense, that is exactly what the emergency, military, and law enforcement community has been doing since 9/11—searching out the best approach and adapting to the new reality. As law enforcement and fire personnel perished in the rubble of

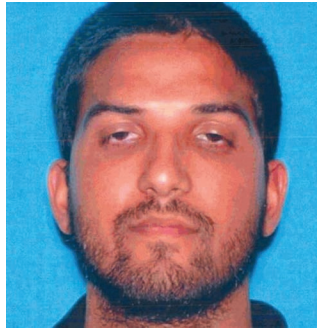


Figure 2.9 California DMV Photo: Rizwan Farook.

the Twin Towers and civilians in the airplanes plummeted to their deaths, the knowledge base of traditional safety was turned on its head.

Soon after 9/11, law enforcement and intelligence agencies developed and learned new strategies and tactics for prevention and mitigation. The safety community began to reevaluate long-established practices in light of this tragedy. From September 11, 2001, an extraordinary series of new approaches was implemented, many of which were implemented by a new DHS. Right from the start, state, local, and federal services rattled the cages of ordinary bureaucratic practices. Getting to the implementation of DHS did not happen overnight but evolved from a series of policy steps. From that tragic day until the following year, government moved at lightning speed, as evidenced by the actions during the month of September 2001 in the chart in Figure 2.10.¹⁴

Not only was a new department erected but so too a new policy and definitional approach. The term *homeland security* encompasses much of the emergency, military, and law enforcement sector once dedicated to a variety of relevant responsibilities involved in the defense of a nation. DHS makes every effort to unify the diverse functions of responsibilities of a homeland in need of protection. DHS is one department chosen over myriad others because DHS is

- One department whose primary mission is to protect the American homeland
- One department to secure our borders, transportation sector, ports, and critical infrastructure
- One department to synthesize and analyze homeland security intelligence from multiple sources
- One department to coordinate communications with state and local governments, private industry, and the American people about threats and preparedness
- One department to coordinate our efforts to protect the American people against bio-terrorism and other weapons of mass destruction
- One department to help train and equip first responders
- One department to manage federal emergency response activities
- More security officers in the field working to stop terrorists and fewer resources in Washington managing duplicative and redundant activities that drain critical homeland security resources¹⁵

As DHS enters its 20th year of operation, the agency clearly has challenges both present and future in scope. DHS has accomplished much over the last two decades, but when reviewing the chronology presented on the pages that follow, try to envision a DHS that might work a bit better or constructed alternatively and with different emphases. Put another way, assume that growth

Homeland Security

in scope and size is not necessarily a good thing but instead, might be a hindrance to better performance. If anything is obvious over the last two decades, it is that DHS has grown in staggering proportions. Growth, in and of itself, is not inevitably a good thing, for critics of DHS often label the agency a “lumbering giant” or a “bureaucratic nightmare” or simply too large to manage in a critically responsive way. DHS must be nimble and quick when dealing with disaster and terror, both the natural and man-made variety. Even the protectors of DHS fully comprehend this fact and that awareness has led to increasing partnerships between DHS and private partners. No better example exists of this cooperative partnership between DHS and the private sector, its industry, security, and emergency services and its intellectual expertise, than is currently playing out in the COVID-19 pandemic. Government alone, nor DHS by itself, could ever solve the pandemic but coupled with private industry, pharmaceutical companies, medical labs, and research facilities, and the pandemic has met its match. As you review the basic historic record of the life of DHS, pose pressing questions in how this agency can retain what it does well and discard what it can never really accomplish. Consider the following policy questions.

September 11
• America attacked • Department of Defense begins combat air patrols over U.S. cities • Department of Transportation grounds all U.S. private aircraft • FEMA activates Federal Response Plan • U.S. Customs goes to Level 1 alert at all border ports of entry • HHS activates (for the first time ever) the National Disaster Medical System, dispatching more than 300 medical and mortuary personnel to the New York and Washington, D.C. areas, dispatching one of eight 12-hour emergency “push packages” of medical supplies, and putting 80 Disaster Medical Assistance Teams nationwide and 7,000 private sector medical professionals on deployment alert. • Nuclear Regulatory Commission advises all nuclear power plants, non-power reactors, nuclear fuel facilities and gaseous diffusion plants go to the highest level of security. All complied. • President orders federal disaster funding for New York • FEMA deploys National Urban Search and Rescue Response team • FEMA deploys US Army Corp of Engineers to assist debris removal
September 12
• FEMA deploys emergency medical and mortuary teams to NY and Washington • FAA allows limited reopening of the nation’s commercial airspace system to allow flights that were diverted on September 11 to continue to their original destinations

Figure 2.10 Homeland Security Administration action during September 2001.

(Continued)

September 13
• President orders federal aid for Virginia • Departments of Justice and Treasury deploy Marshals, Border Patrol, and Customs officials to provide a larger police presence at airports as they reopen
September 14
• President proclaims a national emergency (Proc. 7463) • President orders ready reserves of armed forces to active duty • FBI Releases List of Nineteen Suspected Terrorists
September 17: Attorney General directs the establishment of 94 Anti-Terrorism Task Forces, one for each United States Attorney Office
September 18
• President signs authorization for Use of Military Force bill • President authorizes additional disaster funding for New York
September 20: President addresses Congress, announces creation of the Office of Homeland Security and appointment of Governor Tom Ridge as Director
September 21: HHS announces that more than \$126 million (part of \$5 billion the President released for disaster relief) is being provided immediately to support health services provided in the wake of the attacks.
September 22: President signs airline transportation legislation, providing tools to assure the safety and immediate stability of our Nation's commercial airline system, and establish a process for compensating victims of the terrorist attacks.
September 25: The first of approximately 7,200 National Guard troops begin augmenting security at 444 airports
September 27: The FBI releases photographs of 19 individuals believed to be the 9/11 hijackers

Figure 2.10 (*CONTINUED*) Homeland Security Administration action during September 2001.

1. Which departments or entities were probably not a consistent or operational fit for DHS over its history?
2. Why have so many critics of DHS highlighted the misplacement of the Secret Service within DHS?
3. The United States Coast Guard often finds itself in a cultural and operational contrast to the other workings of DHS. Why is this so?
4. What types of operational activities have been on the rise in DHS?
5. What types of operational activities of DHS have been on the decline or deemphasized?

2.3 DHS: 2001–2003

Any conception of a government agency dedicated to the protection of the homeland takes time to develop and implement. The evolution of a governmental structure, responsible for maintaining homeland safety and security, is both complex and ever changing. Since 2001, the face and internal bureaucratic attributes of DHS have undergone birth and rebirth, change, and reincarnation. The DHS of 2001 was a very different animal from the DHS of today. There have been growing pains in the development of the agency, its mission, and its structure. Despite these challenges, DHS has maintained a unique and surprising adaptability in its changing programs, mission, and structure in its short existence.

MISSION

We will lead the unified national effort to secure America. We will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation. We will secure our national borders while welcoming lawful immigrants, visitors, and trade (U.S. Department of Homeland Security One Team, One Mission, Securing Our Homeland—U.S. DHS Strategic Plan [2008]).

STRATEGIC GOALS

Awareness—Identify and understand threats, assess vulnerabilities, determine the potential impact, and disseminate timely information to our homeland security partners and the American public.

- *Prevention*: Detect, deter, and mitigate threats to our homeland.
- *Protection*: Safeguard our people and their freedoms, critical infrastructure, property, and the economy of our nation from acts of terrorism, natural disasters, or other emergencies.
- *Response*: Lead, manage, and coordinate the national response to acts of terrorism, natural disasters, or other emergencies.
- *Recovery*: Lead national, state, local, and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies.
- *Service*: Serve the public effectively by facilitating lawful trade, travel, and immigration.
- *Organizational excellence*: Value our most important resource, our people. Create a culture that promotes a common identity, innovation, mutual respect, accountability, and teamwork to achieve efficiencies, effectiveness, and operational synergies—U.S. Department of Homeland Security, Securing Our Homeland: U.S. DHS Strategic Plan (2004).

2.3.1 Evolution and Change in DHS

While safety and security issues are permanent national concerns, the examination of how to predict and prevent threats to the national homeland took on added importance after 9/11. On the front burner was how to take existing governmental agencies and deploy them in the fight against terrorism. On the side burner was the nagging question of whether or not the front burner was competent enough to generate the necessary heat and intensity to be successful in this new undertaking. In choosing to erect a new government agency in DHS, both President George W. Bush and Congress agreed that the “changing nature of the threats facing America requires a new government structure against the invisible enemies that can strike with a wide

variety of weapons.”¹⁶ Creating a new agency could be argued as being strictly political—giving the general public a sense of action and aggressive posturing against America’s enemies, although this characterization would be unfair. The previous patchwork of aligned and even competing government agencies was obvious. Even the 9/11 Commission critiqued the lack of information sharing and turf games between competing agencies.

The agencies cooperated, some of the time. But even such cooperation as there was is not the same thing as joint action. When agencies cooperate, one defines the problem and seeks help with it. When they act jointly, the problem and options for action are defined differently from the start. Individuals from different backgrounds come together in analyzing a case and planning how to manage it.

In our hearings we regularly asked witnesses: Who is the quarterback? The other players are in their positions, doing their jobs. But who is calling the play that assigns roles to help them execute as a team?¹⁷

The drive toward a new agency was rooted in a host of compelling rationales. Unity of purpose and mission was surely at the forefront. The “one” agency mindset represented a significant change of ethos for the intelligence community. No longer would the CIA, FBI, National Security Agency (NSA), and North American Aerospace Defense Command (NORAD) see themselves as individual players in the fight against terrorism but instead as part of the collective and simultaneously unified effort to detect and prevent harm to the homeland. DHS refers to these shifts in operational mentality as an “evolution of the paradigm”¹⁸—a movement away from the decentralized toward a totally centralized approach in the management of threat. DHS would be the centerpiece of these efforts.

Not long after 9/11, Congress and the president, working swiftly and in concert, moved passage of the *Homeland Security Act of 2002*.¹⁹ The act seeks to minimize the threat of another 9/11 and poses its mission in broad terms. Part of the act lays out the mission of DHS.

The primary mission of the department is to

- Prevent terrorist attacks within the United States
- Reduce the vulnerability of the United States to terrorism
- Minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States
- Carry out all functions of entities transferred to the department, including by acting as a focal point regarding natural and man-made crises and emergency planning
- Ensure that the functions of the agencies and subdivisions within the department that are not related directly to securing the homeland are not diminished or neglected except by a specific explicit act of Congress
- Ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland
- Monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking²⁰

The act further compartmentalizes the agency into four main areas of responsibility, namely, border and transportation; emergency preparedness and response; chemical, biological, radiological, and nuclear countermeasures; and information analysis and infrastructure protection. The organization chart of DHS in 2008,²¹ shown in Figure 2.11, portrays those with crucial responsibility for DHS.

The significance of these categories cannot be overemphasized. In border and transportation, DHS assumed control over security services relating to our borders, territorial waters, and

Homeland Security

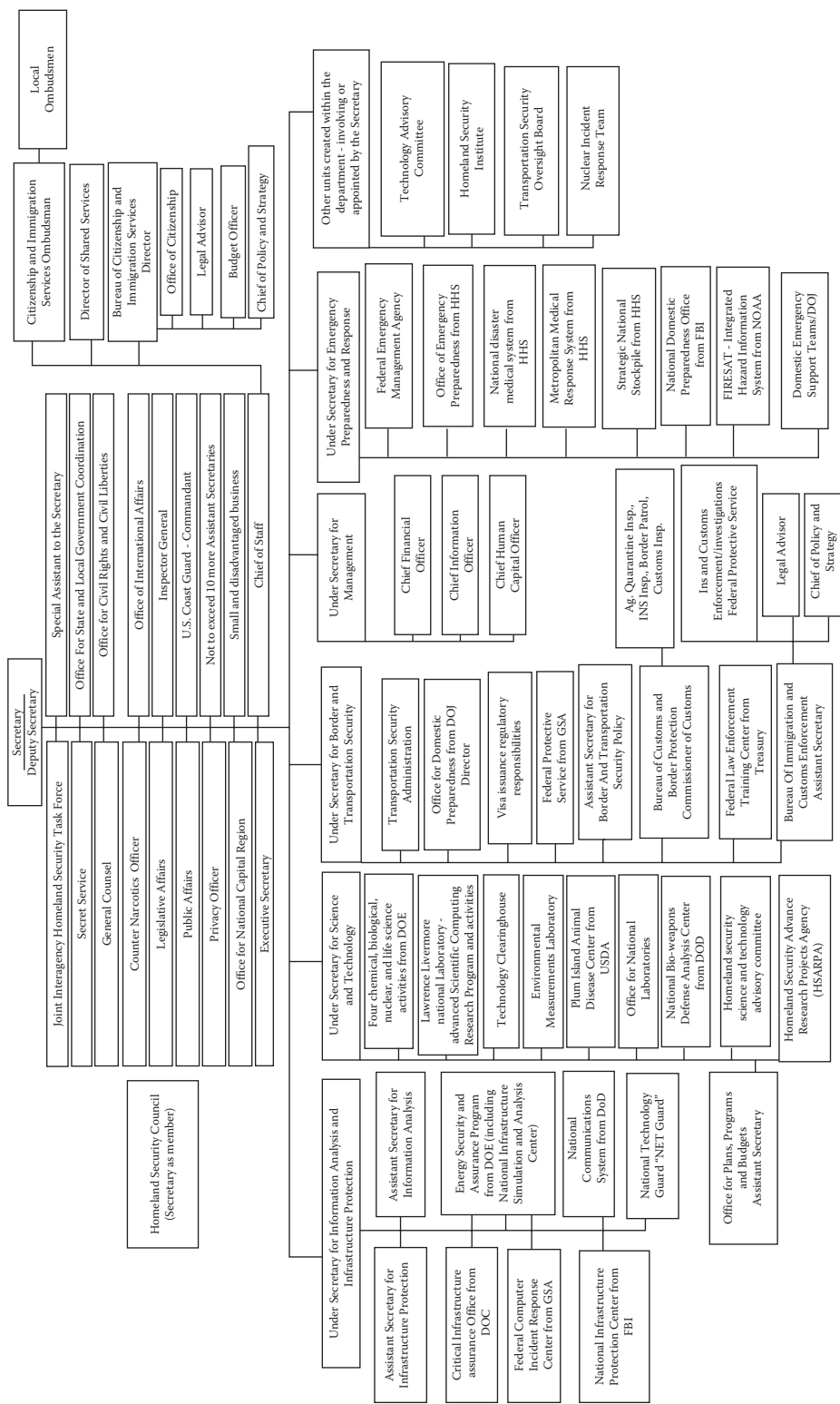


Figure 2.11 DHS organizational chart in 2008.

2.4 Reorganization and Evolution of DHS: 2003–2015

transportation systems. Immigration and naturalization, customs, the coast guard, and animal protection issues are now DHS functions.

In emergency preparedness and response, there was a complete merger of Federal Emergency Management Agency (FEMA) operations into DHS. FEMA, as will be discussed in Chapter 7, became an organization dedicated not only to natural disaster but also to man-made events. Federal interagency emergency programs were subsumed into DHS, as were critical response units relating to nuclear and pharmaceutical events.

In matters involving the prevention of chemical, radiological, and nuclear terror, DHS plays a central, coordinating role. Efforts here would be one of centralization and coordination of diverse department activities across the spectrum of government agencies. Guidelines regarding weapons of mass destruction were rapidly promulgated.

In the area of intelligence and threat analysis, DHS acts as a central repository for information pertaining to threats to the homeland. Data from traditional intelligence organizations such as the CIA, FBI, NSA, the Immigration and Naturalization Service (INS), and the Drug Enforcement Administration (DEA) are catalogued and disseminated as needed. DHS now works closely with the FBI's Office of Intelligence.

As for infrastructure, DHS is responsible for the evaluation and protection of the country's primary infrastructure, including food and water systems; health and emergency services; telecommunications; energy; chemical and defense industries; and common carrier transportation. Issues of infrastructure continue to be pressed by both the executive and legislative branch.

Finally, DHS as of 2003 extended its program reach to state, local, and private sector justice agencies. One of the hallmarks of DHS is the cultivation of governmental inter- and intra-agency cooperation. DHS saw the essential need for mutual trust and respect between competing agencies so that the mission of DHS might be implemented. DHS erected an "intergovernmental affairs office" to coordinate the numerous initiatives emanating from the agency. Figure 6.4 in Chapter 6 contains contact information for state offices dedicated to the affairs of homeland security.

In time, these external constituencies will take on added importance for DHS. Structurally, DHS will have to adapt and evolve to serve these varied interests.

The Homeland Security Act of 2002 also mandated:

Not later than 60 days after enactment, of a reorganization plan regarding two categories of information concerning plans for DHS ("the Department" or "DHS"):

The transfer of agencies, personnel, assets, and obligations to the Department pursuant to this Act.

Any consolidation, reorganization, or streamlining of agencies transferred to the Department pursuant to this Act.²²

Internet Exercise: For the complete text of the Homeland Security Act of 2002, see http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

2.4 Reorganization and Evolution of DHS: 2003–2015

In accordance with the act, DHS looks internally and externally for structural changes within the agency and the merger of agencies from outside. The task of DHS is to foster the unified culture of prevention and information sharing so needed in the fight against terrorism. DHS is many things to many entities, and, in the final analysis, it is a clearinghouse as well as an operational center for policy on homeland safety and security. DHS minimally

- Prevents terrorist attacks within the United States
- Reduces America's vulnerability to terrorism
- Minimizes the damage and oversees the recovery from attacks that do occur²³

The 2015 structure of DHS is charted in Figure 2.12.

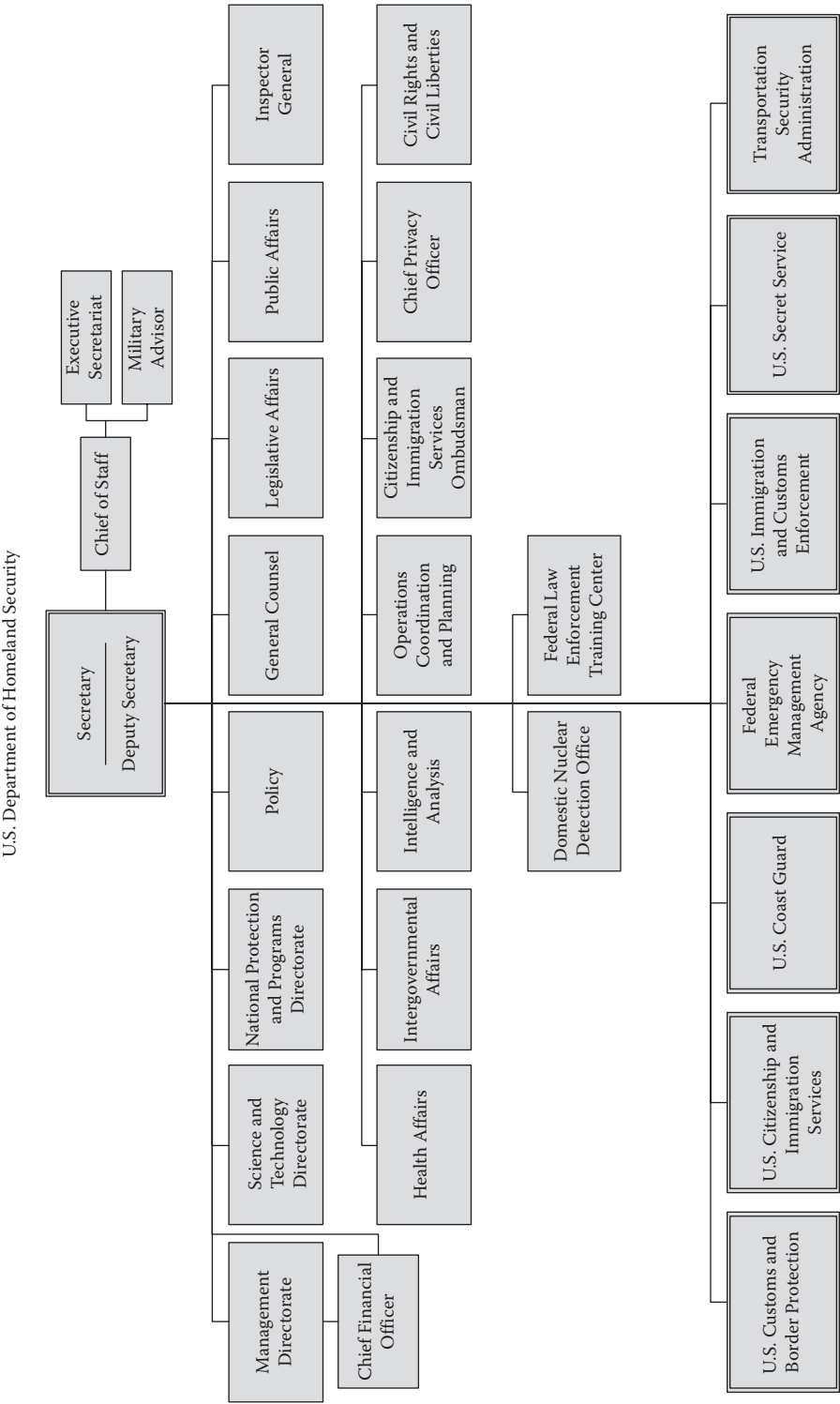


Figure 2.12 DHS organizational chart as of August 25, 2015. (<https://www.dhs.gov/sites/default/files/publications/dhs-orgchart.pdf>.)

2.5 DHS in the Age of President Donald J. Trump: 2016–2021

Over its short life span, DHS has evolved vigorously, at least in a programmatic sense, but it has taken to a slow mode of structural change. From 2008 to the present, the structure of DHS displays only minor internal and administrative differences.

For example, the National Cyber Security Center no longer stands side by side with the Federal Law Enforcement Center and Domestic Nuclear Detection Office but has been merged into the DHS Directorate on Science and Technology. Replacing the National Cyber Security Center, as a stand-alone office, is Intergovernmental Affairs. For the remainder, the 2008 version of DHS is identical to that promulgated in 2001. Given the previous “sweeps” of agencies and personnel, it is likely the prudent course, which ensures stability. Even so, there are many legislators and policymakers who have urged some significant consolidation and merger of task and function at DHS and budget realities may force that issue in the very near future.²⁴

2.5 DHS in the Age of President Donald J. Trump: 2016–2021

Since the election and installation of Donald J. Trump as the 45th President of the United States, DHS could be accurately described as operating in a whirlwind. There are various reasons for this. First, was the operational and managerial style of Trump who insisted on high levels of loyalty without fail and the advancement of his DHS agenda. In each of these cases, the agency had never encountered the likes of President Trump for his managerial style can be termed frenetic. Couple this with his firm demand that his team players be on his team resolutely and unequivocally, and you have a cultural dynamic the agency never previously encountered. Mostly, however, President Trump saw the basis of election rooted in many aspects of what DHS does, such border security, immigration, border wall construction, and putting American companies and workers first. To say there was a systematic shake-up at DHS is an understatement. See the current US Department of Homeland Security Organization Chart at Figure 2.13.²⁵

2.5.1 Office of the Secretary of DHS

Within DHS, the organizational structure of the Office of the Secretary was altered under the provisions of the act. The secretary of homeland security oversees and provides leadership in all facets of homeland defense and protection.

U.S. Department of Homeland Security

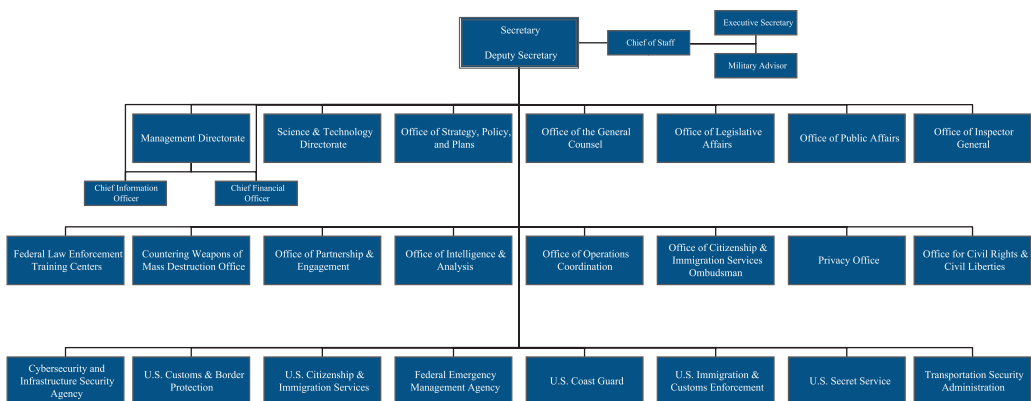


Figure 2.13 The current DHS Organization Chart by position.

Homeland Security



Figure 2.14 Tom Ridge, the first Secretary of the Department of Homeland Security. (From Department of Homeland Security, Washington, D.C.)



Figure 2.15 Michael Chertoff, Homeland Security Secretary 2005–2009. (From Department of Homeland Security, Washington, D.C.)

During its early history, the secretary was Thomas Ridge former Pennsylvania governor (Figure 2.14).

Secretary Ridge is largely lauded for his skill and demeanor during the turbulent initial days of DHS. His reputation for integrity, consensus building, and political skill is well deserved.

After Secretary Ridge, the leadership of DHS was provided by former prosecutor and judge Michael Chertoff (Figure 2.15).

Secretary Chertoff was a tireless advocate for his department. His six-point agenda for DHS, developed and announced in July 2005, ensures that the department's policies, operations, and structures are aligned in the best way to address the potential threats—both present and future—that face the United States. The agenda for DHS includes these tenets:

- Increase overall preparedness, particularly for catastrophic events
- Create better transportation security systems to move people and cargo more securely and efficiently

2.5 DHS in the Age of President Donald J. Trump: 2016–2021



Figure 2.16 Janet Napolitano, the third Secretary of Homeland Security. (From Department of Homeland Security, Washington, D.C.)

- Strengthen border security and interior enforcement and reform immigration processes
- Enhance information sharing with our partners
- Improve DHS financial management, human resource development, procurement, and information technology
- Realign the DHS organization to maximize mission performance

With the election and swearing in of Barack Obama, the 44th president of the United States, a new homeland security secretary was confirmed and appointed. Janet Napolitano (Figure 2.16) was sworn in on January 21, 2009, as the third secretary of DHS.

Napolitano's homeland security background was extensive. As U.S. attorney, she helped lead the domestic terrorism investigation into the Oklahoma City bombing. As Arizona attorney general, she helped write the law to break up human smuggling rings. As Governor of Arizona, she implemented one of the first state homeland security strategies in the country, opened the first state counterterrorism center, and spearheaded efforts to transform immigration enforcement. She has also been a pioneer in coordinating federal, state, local, and binational homeland security efforts, and presided over large-scale disaster relief efforts and readiness exercises to ensure well-crafted and functional emergency plans.

As the first woman to head up the new agency, the DHS chief's tenure was marked by such notable events as the Christmas Day bombing on December 25, 2009; the shooting attack and assassination attempt on House Representative Gabrielle Giffords and others in Arizona on January 8, 2011; the shooting in a movie theater in Aurora, Colorado, on July 20, 2012; the Sandy Hook Elementary School shooting in Newtown, Connecticut, on December 14, 2012; as well as the Occupy Movement and the tragedy caused by the Boston Marathon bombing on April 15, 2013 (Figure 2.17).

These are in addition to numerous domestic terrorist plots in various stages that had been thwarted by U.S. intelligence agencies within DHS. These events and phenomena, as well as the various plots, obviously influenced the focus of the agency. The secretary's platform emphasized an increased need for utilities security, including supervisory control and data acquisition (SCADA) systems that control utilities, and the need for increased vigilance and expertise in the area of cybersecurity across both the public and private sectors.

Napolitano's tenure as DHS chief was not without controversy. This included various reports of wasteful spending by DHS, certainly something that many government agencies are not immune to. In addition, civil liberties groups decried the continued use of Transportation

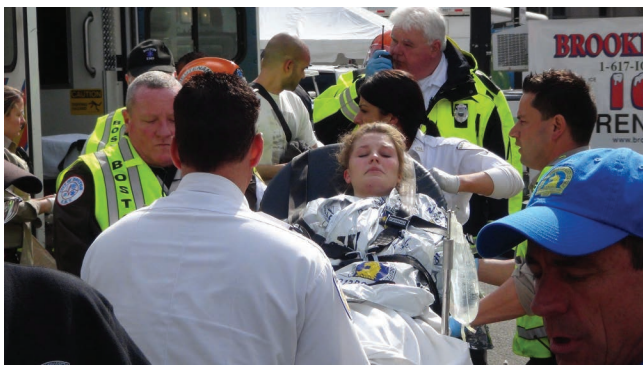


Figure 2.17 Boston, MA, April 15, 2013: Medical teams assist those injured from the bombings at the Boston Marathon. (From FEMA News Photo, Washington, D.C.)

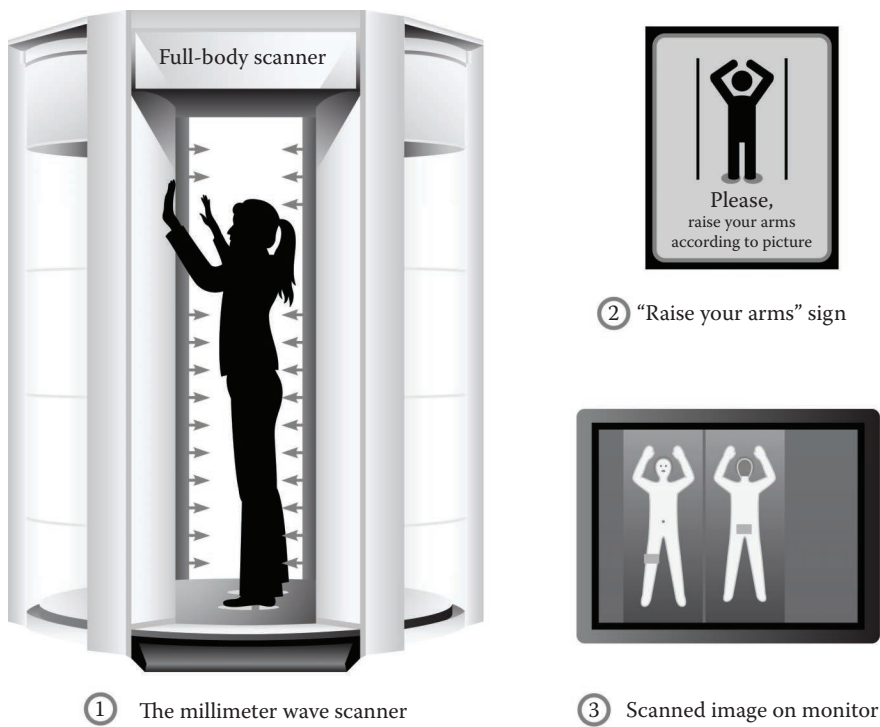


Figure 2.18 Advanced imaging technology (AIT) in use by TSA.

Security Administration (TSA) pat downs and imaging technologies—which some argue are too invasive—in airport security screening²⁶ (see Figure 2.18).

In the wake of the Christmas Day bombing in 2009, the secretary had to backtrack on statements that “the system worked” to concede that the system, in fact, did not work. This is because Umar Farouk Abdulmutallab was allowed to board a plane with explosives and make it all the way to Detroit before his underwear bombing device failed to detonate properly. Reports also indicate that the United States had received intelligence, prior to the attack attempt, in reference to a Nigerian national based in Yemen planning a possible attack.

2.5 DHS in the Age of President Donald J. Trump: 2016–2021



Figure 2.19 Fourth Director of Homeland Security, Jeh Charles Johnson. (From Department of Homeland Security, Washington, D.C.)

Another notable event, no fault of Secretary Napolitano's, was the disclosure of the failed "Fast and Furious" operation, conducted from 2006 to 2011, in which over 1,600 firearms that were sold to dealers ultimately made their way into the hands of Mexican traffickers. The intent was to track the weapons and reveal key figures in the Mexican cartel hierarchy. The operation, however, was a failure in that not only did authorities not track the movement of guns, according to reports, but those guns have been directly linked to over 200 deaths in Mexico. While this originated under the watch of Attorney General Eric Holder—out of the Bureau of Alcohol, Tobacco, and Firearms (ATF) and not DHS—it was perceived as a black-eye moment for the Obama administration, one that tested the public's trust of government operations in the name of security, not to mention an increasingly tense relationship with Mexico. If anything, the operation emphasized the importance of border security in the south and the need to stem the increasing threat of violence spilling over the border from Mexico, albeit not in a wholly positive way. Despite these controversies and the increasing range of threats and challenges, Secretary Napolitano ably led the department on a range of new initiatives.

After Napolitano's tenure, Jeh Charles Johnson, a leader strong on legal preparation and analysis, but with limited actual homeland security experience (see Figure 2.19), was sworn in on December 23, 2013.

While political appointments frequently reflect political realities more than experiential resumes, Jeh Johnson has been at times a polarizing and complex figurehead for DHS. For example, Secretary Johnson has shown general reticence to label terrorist acts as terrorist acts or to use nomenclature such as "jihad" or "Islamic Terrorism." This has led to a debate on political correctness and whether the avoidance of using such valid terminology ignores the issues and undercuts the operational integrity of what DHS must encounter every day. On the other hand, Secretary Johnson gets high marks for his integrity, his willingness to delegate and rely on talented people, and an overall leadership style that keeps the rank and file in DHS in a contented state. Since his tenure ended, his public contributions and insights have highlighted his honest approach and how DHS came to rely on his professional manner. For example, Secretary Johnson has been keenly critical of the politics so evident in the Coronavirus situation and has vociferously asked for a national response rather than a party-based reaction.²⁷ Johnson was equally fair in his assessment of border detention facilities where children and families were cared for but not necessarily at a perfect level. Johnson noted that the sheer volume and the fact these policies were attributable to the Obama administration.²⁸

Secretary Johnson has also called for increased and liberal discretion in the use of resources to deport or detain illegal aliens on American soil. Citing that DHS has only so many resources,

Homeland Security

his office rescinded a host of previous practices dealing with the apprehension, detention, and deportation of illegal aliens and replaced those policies with a priority system, whereby only certain groups would be subject to prosecution and deportation. His “Priority 1” grouping was as follows:

Aliens described in this priority represent the highest priority to which enforcement resources should be directed:

1. Aliens engaged in or suspected of terrorism or espionage, or who otherwise pose a danger to national security
2. Aliens apprehended at the border or ports of entry while attempting to unlawfully enter the United States
3. Aliens convicted of an offense for which an element was active participation in a criminal street gang, as defined in 18 U.S.C. section 521(a), or aliens not younger than 16 years of age who intentionally participated in an organized criminal gang to further the illegal activity of the gang
4. Aliens convicted of an offense classified as a felony in the convicting jurisdiction, other than a state or local offense for which an essential element was the alien’s immigration status
5. Aliens convicted of an “aggravated felony,” as that term is defined in section 101(a)(43) of the Immigration and Nationality Act at the time of the conviction²⁹

After this priority, the DHS mandate becomes far more lenient in matters of enforcement. And when families and children are involved, Johnson increasingly liberalized processes to ensure the least amount of detention possible. In fact, he concluded that “In short, once a family has established eligibility for asylum or other relief under our laws, long-term detention is an inefficient use of our resources and should be discontinued.”³⁰

Finally, Johnson has drawn criticism for advancing a theory of racial profiling at border enforcement relative to drug enforcement, especially at the Mexican border.

Despite some controversies, which go with the territory, Secretary Johnson successfully oversaw the establishment of policy, procedure, and protocols in the summer and fall of 2014, to identify travelers for screening in response to the Ebola crisis in West Africa. Overall, the department has undergone some significant changes in the several years under his watch.

Internet Exercise: Read Secretary Jeh Johnson’s 2015 progress report on DHS at <https://www.dhs.gov/DHSin2015>.

Within DHS, no matter who the secretary is, he or she orchestrates a complex bureaucracy, like most entities in federal and state service. Many DHS functions are operational and legal in design. Currently, the following departments directly answer to the secretary of DHS:

- *Privacy Office:* Balances and implements privacy laws relevant to DHS action
- *Office of the Inspector General:* Audits, investigates, and inspects practices and protocols of DHS
- *Office of Civil Rights and Civil Liberties:* Delivers legal and policy advice to management at DHS as to practice and constitutional implications
- *Citizenship and Immigration Services Ombudsman:* Resolves individual and employer disputes regarding immigration practices
- *Office of Legislative Affairs:* Liaison with congressional leaders, staff, and the executive branch
- *Office of General Counsel:* Staff of 1,700 lawyers working in the Office of the Secretary as well as the various departments and divisions of DHS

2.5 DHS in the Age of President Donald J. Trump: 2016–2021

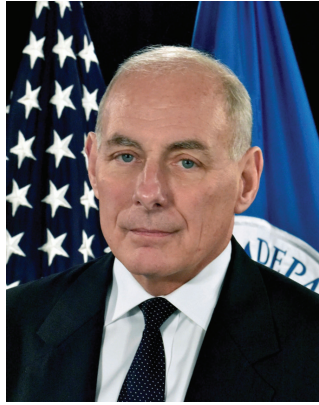


Figure 2.20 General John Kelly (From Department of Homeland Security, Washington, D.C.)

Other offices include Public Affairs, Military Advisor's Office, Counter Narcotics Enforcement, and the Executive Secretariat. Of recent interest is September 28, 2015, announcement of a new Office of Community Partnerships. The office targets the increasing caseload of domestically generated violent extremism, hoping to build bridges between DHS and community groups aware of domestic terror plots but fully in opposition to those approaches. This office will be dedicated to the mission of countering violent extremism and developing community partnerships that will combat and ferret out these threats.³¹

In the span of 3 years, since 2016, the Trump Administration had four DHS Secretaries. Former Marine General John Kelly was President Trump's first choice to lead the DHS. Kelly brought systematic order to an agency being pulled in diverse directions and his military leadership style was very beneficial to the department especially when one considers the political pressures applied to it on so many levels. See Figure 2.20.

Secretary Kelly's leadership capabilities are well known and equally well respected. His impact and changes to the agency work are as follows:

1. Change of command and staff officers that acted in contravention to the President's DHS outlook
2. Encouraged and supported stronger border protection policies and practices
3. Affirmed neglected immigration policies that favored US workers over visa workers
4. Stressed the "merit-based" immigration policy over the open-door policy to any party seeking refuge in the United States
5. Correlated border policy with drug policy since he recognized the connectivity of the two issues
6. Enforced time limitations on "Temporary Protected Status" entrants
7. Worked to increase of deportation of those overstaying their visas
8. Correlated and enacted policies that understood the connection between border controls and terrorist groups and activities

In general, General Kelly adopted a harder line on border security fully consistent with the policies of the Trump administration. Secretary Kelly subsequently assumed the role of Chief of Staff for President Trump and his role while short in duration was marked by a very successful managerial and operational style.



Figure 2.21 DHS Secretary Kirstjen Nielsen. (From Department of Homeland Security, Washington, D.C.)

Next, President Trump appointed Kirstjen Nielsen (Figure 2.21) as Secretary from 2017 to 2019.

Secretary Nielsen worked her way up and through the ranks of DHS and worked very effectively with General John Kelly. A tireless leader and a strong advocate of stricter border policies, Secretary Nielsen labored in very difficult times for DHS. Essentially, her performance was largely shaped by enforcement of the “Zero-Tolerance Policy” whereby illegal immigrants caught at the border were immediately referred for criminal prosecution. And while that policy might have been legal and justified, the image problems of the policy are now legendary—the most illustrative example being how children could be separated from their illegally crossing parents, or from caretakers incorrectly or improperly claiming “asylum.” Efforts to enforce the policy ignited a firestorm of protest over its inhumanity rather than legality, although various federal courts intervened in questionable ways to make that policy difficult to enforce.³²

Secretary Nielsen often used controversial measures such as the firing of tear gas when civil disturbances at the border became more commonplace. While there were undeniably a host of critics, there were supporters as well. No Secretary of the DHS can withstand withering criticism, but in Secretary Nielsen’s case, her tenure was marked by torrid, competing headwinds.³³

While her tenure was, at times, rancorous, Secretary Nielsen delivered some significant accomplishments including:

- A renewed emphasis on the cyber-security challenges
- Establishment of a National Risk Management Center in New York City dedicated to cyber challenges
- DHS Technology Updates in Training and Equipment for Cyber Challenges
- Voter and Election Protocols and Measures to Reduce Foreign Interference and Fraud

Next, President Trump appointed Acting Secretary Kevin K. McAleenan in 2019 (Figure 2.22).

As former Commissioner of the U.S. Customs and Border Patrol, Secretary McAleenan brought strong experiential qualifications to his position. As already evident, the appointment of DHS Secretary is often political exercise more than any other measure. McAleenan brought a wealth of experience when assuming this post. As CBP’s chief executive, McAleenan oversaw 60,000 employees, managed a budget of over \$13 billion, and ensured the effective operations of CBP’s mission to protect national security while promoting economic prosperity.

2.5 DHS in the Age of President Donald J. Trump: 2016–2021



Figure 2.22 Acting DHS Secretary Kevin K. McAleenan. (From Department of Homeland Security, Washington, D.C.).

While McAleenan's tenure was only a year, his contributions to the vision and outlook of DHS were quite significant. His most important leadership approach forced DHS to look within our borders rather than gazing to other countries or overseas. While terror often comes or generates from foreign countries, the preparation and training may be home-grown or domestic. This operational approach is fully described in the DHS Factsheet (Figure 2.23).³⁴

As Acting Secretary, McAleenan continued the pursuit of overseas terrorists but targeted domestic actors that could wreak havoc on our homeland. As part of the revised strategic framework of the department, DHS reprioritized and re-emphasized things.³⁵ His revision of the DHS Strategic Framework stressed the following goals:

- Understand the evolving terrorism and targeted violence threat environment, and support partners in the homeland security enterprise through this specialized knowledge.
- Prevent terrorists and other hostile actors from entering the United States, and deny them the opportunity to exploit the Nation's trade, immigration, and domestic and international travel systems.
- Prevent terrorism and targeted violence.
- Enhance U.S. infrastructure protections and community preparedness.

Secretary McAleenan's very short tenure as DHS Secretary was not caused due to major policy differences with the Trump administration but the difficulties of traversing the fluid political realities of the position. After a long and distinguished career, McAleenan indicated it was time to be closer to family and to spend some time in the private sector. President Trump was very commendatory of his service but rumors swirl about whether the President thought he was aggressive enough in implementing his border policies.³⁶

The appointment of Chad Wolf to Acting Secretary in 2019 by President Trump (Figure 2.24) represented the fourth Trump appointee to the post, and the second longest tenured DHS head after Nielsen.

To say there has been tumult at DHS is an understatement. In an agency so fractured and disjointed by its inherent complexity, the transiency of its appointed or Congressionally approved Secretaries provides little stability to the department. And while all the Secretaries under the Trump administration have made valuable contributions to the role and functions of the department, it was hoped the appointment of Chad Wolf might calm the turbulence a bit. Secretary Wolf was Chief of Staff to former Secretary Kirstjen Nielsen; Assistant Secretary of

Homeland Security for Strategy, Plans, Analysis & Risk as well as Under Secretary for this same, crucial office. Wolf was not without controversy including a rejection of New York State's right to participate in the "Global Entry" program because the state will not allow access the DMV records to check backgrounds of the applicants.

U.S. DEPARTMENT OF HOMELAND SECURITY

FACT SHEET: DHS Strategic Framework for Countering Terrorism and Targeted Violence

INTRODUCTION

The U.S. Department of Homeland Security was created in the wake of the devastating 9/11 attacks to coordinate and unify the nation's homeland security efforts. As we marked the 18th anniversary of the attacks, the country confronts an evolving challenge of terrorism and targeted violence.

Foreign terrorist organizations remain a core priority of DHS's counterterrorism efforts and we will continue to make substantial progress in our ability to detect, prevent, protect against, and mitigate the threats that these groups pose. At the same time, we face a growing threat from domestic terrorism and targeted violence here at home. We must address and prevent the mass attacks that have too frequently struck our houses of worship, our schools, our workplaces, our festivals, and our shopping spaces.

DHS is introducing a new document, DHS Strategic Framework for Countering Terrorism and Targeted Violence, which explains how we will use the tools and expertise that have protected and strengthened the country from foreign terrorist organizations to address the evolving challenges of today.

- DHS was founded after the 9/11 attacks with the mission of safeguarding the country from threats, foreign and domestic.
- Nearly two decades after the attacks, the U.S. faces an increasingly complex and evolving threat of terrorism and targeted violence.
- Since its inception, DHS has developed and implemented an array of tools to address threats to the nation.
- DHS is rolling out a new Strategic Framework for combating terrorism and targeted violence that will make it clear that the whole of DHS is committed to addressing the threat posed by terrorism and targeted violence at home, just as we are committed to addressing the threat posed by foreign terrorist organizations.
- The Strategic Framework takes a whole-of-society approach to prevention, empowering our citizens and our state, local, tribal, and territorial authorities, as well as our private sector, non-governmental, and community leaders, to develop localized prevention frameworks to protect their communities. By empowering our homeland security enterprise, DHS will continue to adapt ahead of evolving threats, enhancing the safety of our nation.



**Homeland
Security**

Figure 2.23 DHS's Strategic Framework Fact Sheet. (From Department of Homeland Security, Washington, D.C.)

(Continued)

2.5 DHS in the Age of President Donald J. Trump: 2016–2021

Current and Emerging Threats:

- Just like when DHS was founded, foreign terrorist organizations remain intent on striking the country through directed attacks or by radicalizing the most vulnerable and disaffected Americans.
- These groups seek to spur to violence our youth, our disenfranchised, and our disaffected—encouraging them to strike the heart of our nation and attack the unity of our vibrant, diverse society.
- ISIS, al Q'aida, returning foreign fighters, and those still in prison in theater represent significant, persistent, and long-term national security threats.
- Today, we face a growing threat from domestic actors inspired by violent extremist ideologies, as well as attacks from those are not ideologically driven.
- The prevalent trend of Americans driven by violent extremist ideologies or personal grievances to commit acts of terrorism and targeted violence with little apparent warning creates a unique challenge to traditional law enforcement and investigation methods.
- Racially- and ethnically-motivated violent extremism, in particular, violent white supremacism, is one of the most prevalent and abhorrent of these anti-American ideologies. There is no moral ambiguity on this issue.



GOALS OF THE STRATEGY

Goal 1: Understand the evolving terrorism and targeted violence threat environment and support partners in the homeland security enterprise through this specialized knowledge.

Goal 2: Prevent terrorists and other hostile actors from entering the United States, and deny them the opportunity to exploit the nation's trade, immigration, and domestic and international travel systems.

Goal 3: Prevent terrorism and targeted violence.

Goal 4: Enhance U.S. infrastructure protections and community preparedness.



Homeland
Security



DHS STRATEGY AND ACTIONS

- This is the first national-level strategy to explicitly state that terrorism and targeted violence overlap, intersect, and interact as problems and require a shared set of solutions.
- DHS is introducing new methods of creating a more comprehensive understanding of the challenge of terrorism and targeted violence, both within and outside the federal government.
- The Strategic Framework introduces a new annual assessment that will explicate the state of the threat to the nation. This new report will help to inform all levels of government and the broader public.
- The Strategic Framework also introduces a mechanism for crafting a new definition of the key concept of targeted violence and elucidates the nature of today's domestic challenges and, in particular, the dangers of violent white supremacism extremism.
- This Strategic Framework is designed to assess DHS's past and provide a guidepost to its future. It lays out a comprehensive framework to enhance our prevention capabilities in an age of complex and multidimensional domestic threats, regardless of ideology.
- Importantly, the Strategic Framework explicitly recognizes the need to focus on and protect our most vulnerable populations, particularly our youth.
- This Strategic Framework emphasizes the importance of transparency, the protections of civil rights and civil liberties, and the protection of data in a digital age.
- The Strategic Framework is intentionally forward-looking in its understanding of technology's role as a factor that can exacerbate problems, but also one that can provide new solutions to combat the threats we confront.
- DHS will follow this strategy with a public action plan, explaining to the American people in greater detail how we will accomplish our strategic goals.
- DHS has dedicated operators and personnel that will play a critical role in implementing this strategy with vigilance and integrity.

Figure 2.23 (CONTINUED) DHS's Strategic Framework Fact Sheet. (From Department of Homeland Security, Washington, D.C.)

Internet Exercise: See the DHS announcement on the New York State restriction at: <https://www.cbp.gov/newsroom/national-media-release/new-york-residents-no-longer-eligible-apply-or-renew-trusted>

In addition, the Secretary supported the use of unmanned technology in the war on terror, especially as it relates to drone use whether at the border, drug interdiction, or maritime protection. See Figure 2.25.³⁷



Figure 2.24 Acting DHS Secretary Chad Wolf. (From Department of Homeland Security, Washington, D.C.)



Figure 2.25 A Border Patrol agent near Tucson, Arizona, readies a fixed-wing drone for launch. Photo by Border Patrol Agent Andrew Franklin. (Source: Customs and Boarder Patrol.)

Secretary Wolf expanded DHS efforts to reconnect all separated families, continued efforts to assure election processes and voting integrity, finished the DHS Strategic Mission and Plans, as well as gave some increased priority to assuring humanitarian treatment of those seeking entry at the borders.³⁸ In September through November 2020, several court rulings determined that Acting Secretary Wolf is likely unlawfully serving as acting secretary of the Department of Homeland Security, due to the fact that appointment was invalid under the agency's applicable order of succession. As such, it may be determined by various court that some policies implemented during his tenure will be invalidated or overturned at some point.

It should be noted that two other individuals served as acting DHS heads at the tail end of Trump's presidency, including Pete Gaynor for nine days and David Pekoske for thirteen days.

Under the Biden Administration, Alejandro Nicholas Mayorkas took over on February 2, 2021 as the seventh DHS Secretary. He served in DHS under the Obama administration both as the director of United Citizenship and Immigration service for four years and as Deputy Secretary for here years under then Secretary Jeh Johnson.

2.5.2 DHS Directorates

In the reorganization phase, DHS clearly articulated its internal structure by establishing a myriad of internal departments. At various stages from 2005 until the present, directorates were implemented and, in some cases, were later abolished. To say that DHS is a dynamic bureaucracy is an understatement. At face value, the directorates reflect the stress of the agency—what it wishes to primarily focus on. Before 2005, during reorganization, directorates were established in

- Border and transportation security
- Emergency preparedness and response
- Information analysis and infrastructure protection

By 2007, each of these directorates was abolished and the respective obligations and duties transferred to other departments within DHS. Currently, there are only two remaining directorates at DHS, although the National Protection and Program Directorate has evolved to an Agency level, and titled Cybersecurity and Infrastructure Security Agency (CISA).

2.5.2.1 Cybersecurity and Infrastructure Security Agency (CISA): Former Directorate for National Protection and Programs

The former Directorate for National Protection and Programs, now labeled CISA—The Cybersecurity and Infrastructure Security Agency, deals with risks to critical infrastructure both physical and virtual threats and dedicates itself to the analysis, identification, and elimination of risk, whether man-made or natural in design. See Figure 2.26.

CISA covers risk from a definitional, cyber, communications, operational, and personnel perspective and stresses best practices to protect infrastructure, both physical and cyber assets, as well as human capital. This included extensive efforts performed overseeing security for the 2020 elections. See Figure 2.27.³⁹

Its modern stress clearly relates to the emerging and unceasing threats to cyber assets but equally the newly formed agency has taken on the role of information source on the COVID-19 pandemic and even particularized guidance on how workers stationed at critical infrastructure need to be protected from the virus. See Figure 2.28.⁴⁰

Internet Exercise: Discover the many roles and functions of CISA at: <https://www.cisa.gov/>

CISA's National Cybersecurity and Communications Integration Center ensures the integrity of governmental and private communications system in order that these systems are free from cyber vulnerabilities. Crucial mission activities of the NCCIC are:

- Information exchange,
- Training and exercises,



Figure 2.26 CISA seal.

Homeland Security



Comprehensive Cyber Protection

CISA's National Cybersecurity and Communications Integration Center (NCCIC) provides 24x7 cyber situational awareness, analysis, incident response and cyber defense capabilities to the Federal government; state, local, tribal and territorial governments; the private sector and international partners.

CISA provides cybersecurity tools, incident response services, and assessment capabilities to safeguard the networks that support the essential operations of federal civilian departments and agencies.



Infrastructure Resilience

CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.

CISA provides consolidated all-hazards risk analysis for U.S. critical infrastructure through the National Risk Management Center.



Emergency Communications

CISA enhances public safety interoperable communications at all levels of government, providing training, coordination, tools and guidance to help partners across the country develop their emergency communications capabilities.

Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters.



National Risk Management Center

The NRMCM is a planning, analysis, and collaboration center working to identify and address the most significant risks to our nation's critical infrastructure.

The NRMCM works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: Identify; Analyze; Prioritize; and Manage the most strategic risks to our National Critical Functions.

Figure 2.27 CISA's Program focus.



Figure 2.28 CISA outlines essential critical workers during the COVID-19 pandemic.



Figure 2.29 DHS Cyber Storm participants, September 2010. (www.dhs.gov.)

- Risk and vulnerability assessments,
- Data synthesis and analysis,
- Operational planning and coordination,
- Watch operations, and
- Incident response and recovery.

CISA plays a crucial role in training and simulation for governmental and private officers entrusted with communication and cyber responsibilities.⁴¹ CISA's *Cyber Storm* exercise provides a biannual opportunity to test and confirm the integrity of communication and cyber designs (see Figure 2.29).

Cyber Storm participants perform the following activities:

- Examine organizations' capability to prepare for, protect from, and respond to cyber attacks' potential effects
- Exercise strategic decision-making and interagency coordination of incident response(s) in accordance with national-level policy and procedures
- Validate information-sharing relationships and communications paths for collecting and disseminating cyber-incident situational awareness, response, and recovery information.
- Examine means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or national security interests⁴²

Central to CISA's overall mission is the protection of the infrastructure, both critical and cyber in design, that includes but is not limited to the power grid, food and water supplies, national monuments, transportation systems, and chemical facilities. Infrastructure sectors include:

- Agriculture and food
- Banking and finance
- Chemical
- Commercial facilities
- Critical manufacturing

Homeland Security

- Dams
- Defense industrial base
- Drinking water and water-treatment systems
- Emergency services
- Energy
- Government facilities
- Information technology
- National monuments and icons
- Nuclear reactors, materials, and waste
- Postal and shipping
- Public health and health care
- Telecommunications
- Transportation systems

CISA analyzes these critical forms of infrastructure to determine potential threats and vulnerability, management, and mitigation of identified risks to same and be just as adept in the coordination of agency response in the event of threat. Covered later in this chapter will be the protocol and methodology of infrastructure analysis. Much of what state, local, and federal authorities do in response to infrastructure threat is derived from the directorate's research results and recommended best practices.

A myriad of other functions assumed by CISA and will be encountered throughout the remainder of this chapter. Increasingly, the department has been given oversight over biometric identity program by and through its office of The Office of Biometric Identity Management (OBIM) which oversees the US-VISIT program and other identity programs. Other offices, such as the National Risk Management Center (NRMC), deal with matters of risk analysis, assessment, and management as well as the emerging statistical and quantitative discipline of risk analytics. The NRMC brings the private sector, government agencies, and other key stakeholders together to identify, analyze, prioritize, and manage the most significant risks to our critical infrastructure. See Figure 2.30.⁴³

2.5.2.2 Directorate for Science and Technology

The role of science and technology in the world of homeland security is patently obvious. As government agencies and localities deal with shrinking budgets, the efficiency and efficacy of their practices take on added importance. The Science and Technology Directorate plays a key role in the development of all forms of technology and scientific applications useful to homeland defense. See the organizational chart in Figure 2.31.⁴⁴



Figure 2.30 NRMC's process to manage risk.

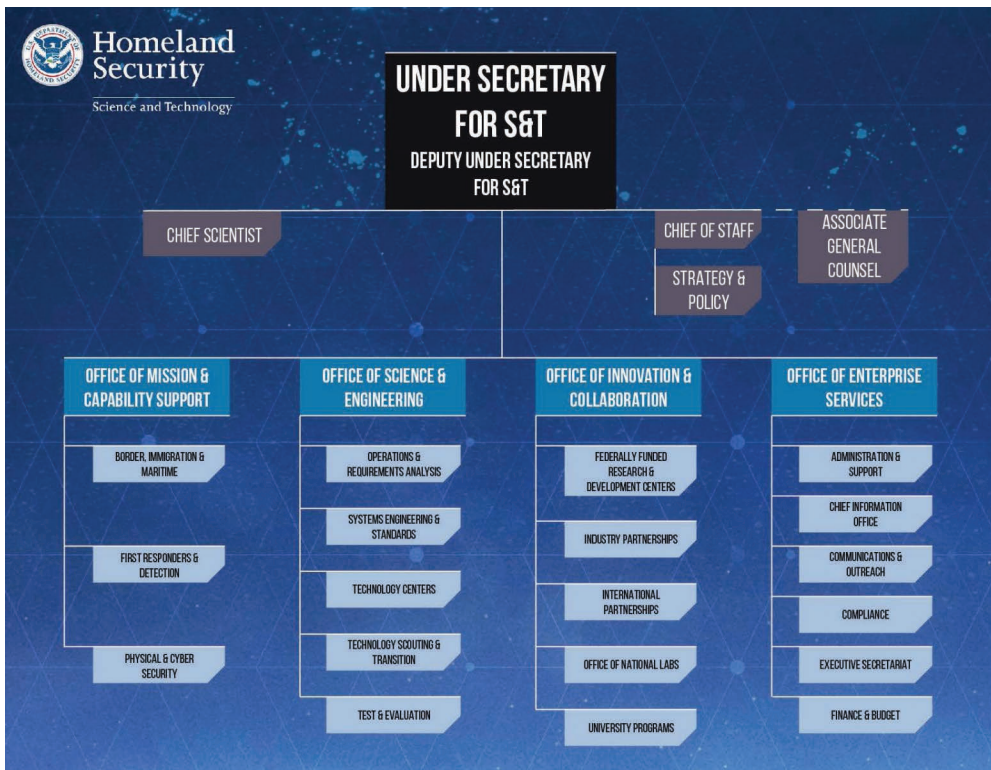


Figure 2.31 DHS's ST&T organizational chart by function and role.

It serves a variety of broader functions, such as being a clearinghouse for technology practices and equipment, especially as to design and engineering; it tests and evaluates the compatibility and interoperability of diverse technologies used across the various states and weighs and assesses the primary needs of the nation's first-responder requirements for technology. The Directorate has played an aligned role in the pandemic Coronavirus by evaluating the surface life of the virus, the impact of ultraviolet light, and other forces which might work toward eradicating this pandemic.⁴⁵

Internet Exercise: Find out how DHS is tackling the pandemic problem at: <https://www.dhs.gov/science-and-technology/blog/2020/04/27/st-finding-ways-fight-covid-19>

The Directorate encompasses the following divisions:

- *Borders and maritime security:* Enhancing security at our nation's borders and waterways without impeding the flow of commerce.
- *Chemical and biological defense:* Detecting, protecting against, responding to, and recovering from chemical and biological incidents.
- *Critical infrastructure and resilience:* Improving the nation's preparedness for natural and man-made catastrophes.
- *Cybersecurity:* Contributing to a safe, secure, and resilient cyber environment.
- *Explosives:* Protecting citizens and infrastructure from the devastating effects of explosives.
- *First responders:* Expanding first responder capabilities and improving their effectiveness, efficiency, and safety.⁴⁶

Homeland Security

The Directorate also engages technology in specific situations such as border and maritime, chemical and biological defense, explosive mitigation, and cybersecurity threats. Among many other activities, the Directorate plays a key role in science and technology development at the college and university level and coordinates a wide array of research and disseminates funds for technological and scientific innovation.

Internet Exercise: Discover the many activities of the Office of University Programs at: <https://www.dhs.gov/science-and-technology/office-university-programs>

2.5.2.3 Directorate for Management

The Directorate for Management is the administrative arm of DHS where traditional functions of personnel, finance, and capital and procurement requirements are dealt with as well as the acquisition and maintenance of DHS properties. The Directorate is responsible for budget development and oversight. With more than 200,000 employees in DHS, the management directorate takes on a major undertaking in the matter of human and physical capital. See Figure 2.32⁴⁷ for the organizational chart of the directorate.

Just moved within the supervision of the Management Directorate is the Federal Protective Service which protects federal assets and installations. The Directorate oversees the activities of the Federal Protective Service (FPS), which is a law enforcement entity dedicated to safety and risk reduction at federal installations (see Figure 2.33).

With more than 2,000 officers and in coordination with a host of contract security firms, the FPS provides security at courthouses, federal buildings, and installations as well as conducting facility assessments and special events protection. The FPS will conduct criminal investigations if required. The FPS provides security services to all federal buildings, including office buildings, courthouses, border stations, and warehouses.

Internet Exercise: Find out about the many careers in the FPS service at: <https://www.dhs.gov/homeland-security-careers/careers-federal-protective-service>

FPS services include but are not limited to:

- Providing a visible uniformed presence in our major federal buildings
- Responding to criminal incidents and other emergencies

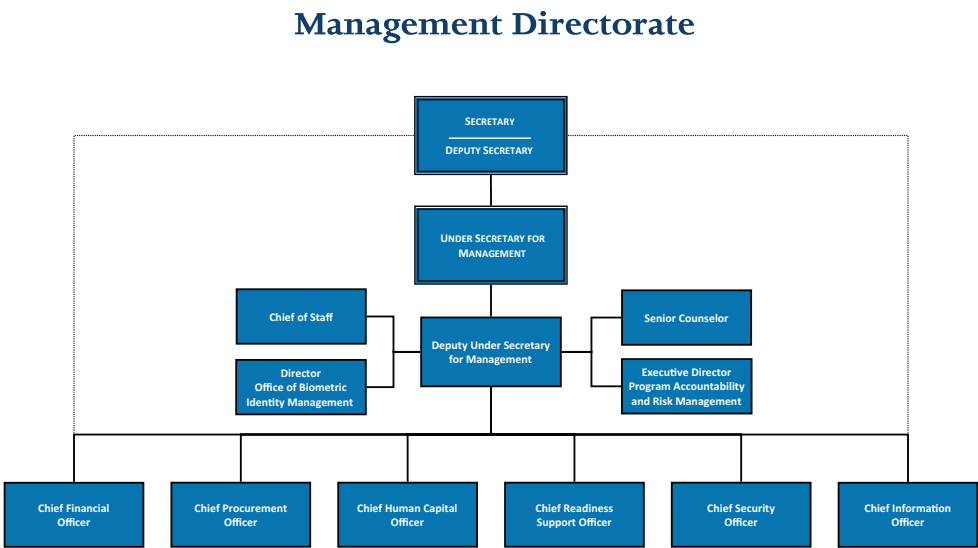


Figure 2.32 DHS Director for Management organizational chart.



Figure 2.33 Federal Protective Service logo.

- Installing and monitoring security devices and systems
- Investigating criminal incidents
- Conducting physical security surveys
- Coordinating a comprehensive program for occupants' emergency plans
- Presenting formal crime prevention and security awareness programs
- Providing police emergency and special security services during natural disasters such as earthquakes, hurricanes, and major civil disturbances—as well as during man-made disasters, such as bomb explosions and riots

The FPS also takes a lead role in the assurance that federal buildings and installations are rid of security problems and that the design, operation, and layout of facilities are as conducive as possible to safe security practices. In each facility, the FPS sets up a Building Security Committee, which conducts a vulnerability assessment of each facility.

Internet Exercise: For a copy of the FPS brochure *Making Buildings Safe*, see <http://www.cdc.gov/niosh/topics/emres/pdfs/FedBuildSafe.pdf>.

2.5.3 DHS Offices: Support and Operational Components

As a complex bureaucracy, DHS never remains organizationally stagnant but appears endlessly capable of growth and transformation. One of the challenges reporting on DHS offices and structure regards their lack of permanency.⁴⁸ DHS subsumes agencies, directorates, divisions, and in carrying out its overall mission, establishes a host of offices- and of recent description what it terms “Support and Operational Components.” Just as the idea of the “Directorate” seems to be shrinking, with only two remaining, the concept of an “Office” seems subject to redesignation and definitional change. DHS’s Support and Operational Components are charted in Figure 2.34.⁴⁹

At the office level, DHS list only three entities:

1. Mass Destruction Office
2. Office of Intelligence and Analysis
3. Office of Operations Coordination

Each of these Offices is described in Figure 2.34.

Homeland Security

United States Coast Guard (USCG)
The United States Coast Guard is one of the five armed forces of the United States and the only military organization within the Department of Homeland Security. The Coast Guard protects the maritime economy and the environment, defends our maritime borders, and saves those in peril.



U.S. Citizenship and Immigration Services (USCIS)
U.S. Citizenship and Immigration Services (USCIS) administers the nation's lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values.



Cybersecurity and Infrastructure Security Agency (CISA)
The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to defend critical infrastructure against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow.



United States Customs and Border Protection (CBP)
United States Customs and Border Protection (CBP) is one of the Department of Homeland Security's largest and most complex components, with a priority mission of keeping terrorists and their weapons out of the U.S. It also has a responsibility for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws.



Federal Law Enforcement Training Center (FLETC)
The Federal Law Enforcement Training Center provides career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently.



Federal Emergency Management Agency (FEMA)
The Federal Emergency Management Agency (FEMA) supports our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.



Figure 2.34 A listing of DHS's various Support and Operational components.

(Continued)

 U.S. Immigration and Customs Enforcement	United States Immigration and Customs Enforcement (ICE) United States Immigration and Customs Enforcement (ICE) promotes homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.		United States Secret Service (USSS) The United States Secret Service (USSS) safeguards the nation's financial infrastructure and payment systems to preserve the integrity of the economy, and protects national leaders, visiting heads of state and government, designated sites, and National Special Security Events.
	Transportation Security Administration (TSA) The Transportation Security Administration (TSA) protects the nation's transportation systems to ensure freedom of movement for people and commerce.	 Homeland Security	Management Directorate The Management Directorate is responsible for budget, appropriations, expenditure of funds, accounting and finance; procurement; human resources and personnel; information technology systems; facilities, property, equipment, and other material resources; providing biometric identification services; and identification and tracking of performance measurements relating to the responsibilities of the Department.

Figure 2.34 (CONTINUED) A listing of DHS's various Support and Operational components.

(Continued)

 Homeland Security	Science and Technology Directorate The Science and Technology Directorate is the primary research and development arm of the Department. It provides federal, state and local officials with the technology and capabilities to protect the homeland.	 Homeland Security	Countering Weapons of Mass Destruction Office The DHS Countering Weapons of Mass Destruction Office (CWMD) works to prevent attacks against the United States using a weapon of mass destruction (WMD) through timely, responsive support to operational partners.
 Homeland Security	Office of Intelligence and Analysis The Office of Intelligence and Analysis equips the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe, secure, and resilient.	 Homeland Security	Office of Operations Coordination The Office of Operations Coordination provides information daily to the Secretary of Homeland Security, senior leaders, and the homeland security enterprise to enable decision-making; oversees the National Operations Center; and leads the Department's Continuity of Operations and Government Programs to enable continuation of primary mission essential functions in the event of a degraded or crisis operating environment.

Figure 2.34 (CONTINUED) A listing of DHS's various Support and Operational components.

2.5.4 Agencies and Entities Swept into DHS

Throughout its history, aside from internal machinations that redesign and redesignate the offices, directorates, and sub-entities of DHS, the Department has often witnessed additions and even subtractions from its overall structure. Often termed “reorganization” the Department has displayed some dynamic changes over its short existence. After 2003, a host of external agencies were also swept into DHS during the reorganization phase:

- *Federal Law Enforcement Training Center (FLETC)*: The premier center for professional law enforcement training, located in Glencoe, Georgia
- *U.S. Customs and Border Protection (CBP)*: The agency primarily responsible for the security of our borders
- *U.S. citizenship and immigration services*: Administers the immigration and naturalization adjudication
- *U.S. Immigration and Customs Enforcement (ICE)*: The investigative arm of DHS that identifies and classifies threats at the borders
- *U.S. Coast Guard (USCG)*: Protection of the nation’s ports and waterways
- *FEMA*: Manages hazards and threats and responds thereto
- *U.S. secret service*: Protection of the president, vice president, and other high-level officials; investigates financial crimes
- *Transportation Security Administration (TSA)*: Protects nation’s transportation systems
- *Domestic Nuclear Detection Office*: Coordinates threat response related to nuclear materials

The intent was to combine, blend, and synthesize appropriate agency functions with the appropriate office. For the most part, DHS has remained largely intact since these radical days of reorganization in 2003–2004. It was not only an administrative sweep that took place when these agencies moved from familiar locale to the DHS setting. For both DHS and the incoming agency, a change of outlook and culture was required. By change, one means that a new prioritization of agency function had to occur; the former agency had to inculcate, acclimate, and become part of a new mission and mindset. In a governmental life span, this is a difficult order to fulfill. Even so, it appears that DHS has done a fairly good job integrating so much in such an expeditious fashion.

To truly appreciate these cultural and administrative shifts, one need only look to the moves from one agency to another (Table 2.1).

In DHS, these moves are simply unrivaled in the history of the government—the movement can only be termed radical in scope. Sweeping moves, from so many governmental agencies, are not the stuff of government personality, whether it is local, state, or federal.

In the final analysis, such shifts and mergers were essential to any notion of a “single roof” for homeland security. While many of these former agencies and offices will be covered in other sections of this chapter, this section will significant structural shifts into DHS.

2.5.4.1 U.S. Coast Guard

The placement of the USCG within DHS was considered a radical shift by many, and by some an uncomfortable fit for a military entity, but on closer inspection, it a defensible move. While the Coast Guard has never been part of the Department of Defense, there are increased calls for its proper placement in that environment.⁵⁰ On the other hand, the mission of the Coast Guard, its historical dedication to safety and security in our waterways and coastline makes the agency the perfect complement to DHS (Figure 2.35).

Homeland Security

Table 2.1 Department of Homeland Security Agency Transfers	
Original Agency (Department)	Current Agency/Office
The U.S. Customs Service (Treasury)	U.S. Customs and Border Protection—inspection, border, and ports of entry responsibilities U.S. Immigration and Customs Enforcement—customs law enforcement responsibilities
The Immigration and Naturalization Service (Justice)	U.S. Customs and Border Protection—inspection functions and the U.S. Border Patrol U.S. Immigration and Customs Enforcement—immigration law enforcement: detention and removal, intelligence, and investigations U.S. Citizenship and Immigration Services—adjudications and benefits programs
The Federal Protective Service	U.S. Immigration and Customs Enforcement
The Transportation Security Administration (Transportation)	Transportation Security Administration
Federal Law Enforcement Training Center (Treasury)	Federal Law Enforcement Training Center
Animal and Plant Health Inspection Service (part) (Agriculture)	U.S. Customs and Border Protection—agricultural imports and entry inspections
Office for Domestic Preparedness (Justice)	Responsibilities distributed within FEMA
The Federal Emergency Management Agency (FEMA)	Federal Emergency Management Agency
Strategic National Stockpile and the National Disaster Medical System (HHS)	Returned to Health and Human Services, July 2004
Nuclear Incident Response Team (Energy)	Responsibilities distributed within FEMA
Domestic Emergency Support Teams (Justice)	Responsibilities distributed within FEMA
National Domestic Preparedness Office (FBI)	Responsibilities distributed within FEMA
CBRN Countermeasures Programs (Energy)	Science and Technology Directorate
Environmental Measurements Laboratory (Energy)	Science and Technology Directorate
National BW Defense Analysis Center (Defense)	Science and Technology Directorate
Plum Island Animal Disease Center (Agriculture)	Science and Technology Directorate

(Continued)

2.5 DHS in the Age of President Donald J. Trump: 2016–2021

Table 2.1 (Continued) Department of Homeland Security Agency Transfers

Original Agency (Department)	Current Agency/Office
Federal Computer Incident Response Center (GSA)	US-CERT, Office of Cybersecurity and Communications in the National Programs and Preparedness Directorate
National Communications System (Defense)	Office of Cybersecurity and Communications in the National Programs and Preparedness Directorate
National Infrastructure Protection Center (FBI)	Dispersed throughout the department, including Office of Operations Coordination and Office of Infrastructure Protection
Energy Security and Assurance Program (Energy)	Integrated into the Office of Infrastructure Protection
U.S. Coast Guard	U.S. Coast Guard
U.S. Secret Service	U.S. Secret Service



Figure 2.35 U.S. Coast Guard approaching a cargo ship.

The mission of the USCG is

- *Maritime safety*: To eliminate deaths, injuries, and property damage associated with maritime transportation, fishing, and recreational boating
- *Maritime security*: To protect America's maritime borders from all intrusions by (1) halting the flow of illegal drugs, aliens, and contraband into the United States through maritime routes; (2) preventing illegal fishing; and (3) suppressing violations of federal law in the maritime arena
- *Maritime mobility*: To facilitate maritime commerce and eliminate interruptions and impediments to the efficient and economical movement of goods and people, while maximizing recreational access to and enjoyment of the water
- *National defense*: To defend the country as one of the five U.S. armed services; to enhance regional stability in support of the National Security Strategy, utilizing the coast guard's unique and relevant maritime capabilities
- *Maritime Stewardship Council*: To eliminate environmental damage and the degradation of natural resources associated with maritime transportation, fishing, and recreational boating (Figure 2.36)⁵¹

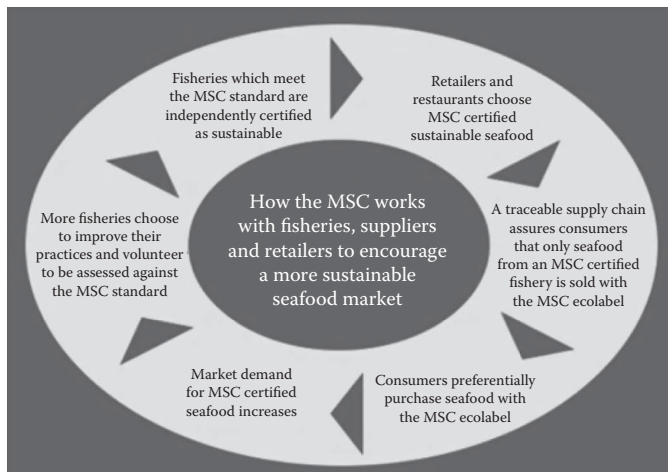


Figure 2.36 Fishing as a sustainable product is part of the USCG's mission.

Long considered a military operation, as one of the five traditional branches in the military complex, the USCG increasingly evolved into a safety and law enforcement organization as well as a military command. How the USCG contributes to the defense of the country is quite evident in its homeland security functions, which include

- Protecting ports, the flow of commerce, and the marine transportation system from terrorism
- Maintaining maritime border security against illegal drugs, illegal aliens, firearms, and weapons of mass destruction
- Ensuring that we can rapidly deploy and resupply our military assets, both by keeping coast guard units at a high state of readiness and by keeping marine transportation open for the transit assets and personnel from other branches of the armed forces
- Protecting against illegal fishing and indiscriminate destruction of living marine resources, and preventing and responding to oil and hazardous material spills—both accidental and intentional
- Coordinating efforts and intelligence with federal, state, and local agencies⁵²

With its extraordinary infrastructure of maritime resources, its skill in the detection and prevention of crime on the seas and waterways, and its technical superiority in a host of operations, the USCG has been called on to be a major player in the fight against terrorism (see Figure 2.37).

The Coast Guard also issues regular, monthly briefings on activity that be deemed suspicious on the maritime front. Each month the Coast Guard posts places and locales that give rise to homeland defense concerns. Figure 2.38⁵³ contains a sample report.

Its flexibility of vision is what makes it a key component of a national strategy. Former Vice Admiral Vivien Crea of the USCG rightfully argues:

The need to protect the homeland in the context of the “long war” against terrorism has been a key force for change in the Coast Guard. Although our initial response to this new terrorism threat temporarily drained resources from other mission areas, we have worked to restore the maritime safety and security mission balance. Congress and the administration have provided critical funding support. New and more capable assets have been added, and all of our resources present a multi-mission capability that can instantly and flexibly surge from search and rescue, to restoration of our ports and waterways, to response to avert threat to our homeland security.⁵⁴



Figure 2.37 New York (September 11, 2001): A Coast Guard patrol boat secures New York Harbor as smoke rises from where the World Trade Center buildings once stood. (From PA2 Tom Sperduto.)

The transition, of course, has not been without its share of challenges. The USCG has a variety of masters to answer to. The sheer volume of coverage, in both task and geography, is daunting. “With 95,000 miles of coastline and close to 360 ports of entry, the United States is challenged daily with monitoring maritime safety, securing national borders and the global supply chain, and protecting natural resources,”⁵⁵ the USCG labors under heavy demands. It has undergone a “fundamental reordering,”⁵⁶ which requires it to be an “instrument of national security.”⁵⁷

2.5.4.1.1 US Coast Guard Auxiliary

Given the increasing demands imposed on the Coast Guard, the Commandant of the Coast has been extending and expanding the role of the Coast Guard’s Volunteer—some 32,000 Coast Guard Auxiliary members who perform a myriad of function on a volunteer basis. See Figure 2.39.

Operating in all 50 states and U.S. Territories, the Auxiliary serves the overall mission of Coast Guard in most activities except direct military conflict or combat. The primary duties of the Auxiliary relate to:

- Safety and Security Patrols
- Search and Rescue
- Mass Casualty or Disasters
- Pollution Response and Patrols
- Homeland Security
- Recreational Boating Safety
- Commercial Fishing and Vessel Exams
- Platforms for Boarding Parties
- Recruit for all service in the Coast Guard

Homeland Security

The Auxiliary is heavily involved in recreational boating safety inspections on all American waterways. Its organizational design consists of the following units:

- *National*: The national staff officers are responsible, along with the Commandant, for the administration and policy-making for the entire Auxiliary.
- *District*: The District provides administrative and supervisory support to Divisions, and promotes policies of both the District Commander and National Committee.

UNCLASSIFIED//FOR OFFICIAL USE ONLY



(U) SCOPE

(U) The Maritime Threat Summary is a monthly product the Maritime Homeland Threat Analysis Branch (MHTAB) of the US Coast Guard (USCG) Intelligence Coordination Center produces for USCG Homeport.^A It highlights suspicious maritime activities and security incidents associated with the US Maritime Transportation System (MTS).

(U) CURRENT TERRORISM THREAT SUMMARY

(U//FOUO) No credible intelligence suggests al-Qa*ida or other transnational terrorist groups are actively plotting attacks against the US MTS; however, they remain the greatest threat. The illicit entry of people and materials into the United States via the maritime domain remains a vulnerability that can be exploited by terrorists.^B

(U) MARITIME THREAT SUMMARY HIGHLIGHTS

(U//FOUO) [GAO Investigators Used Fraudulent TWIC Cards to Access US Seaports, Pg. 3](#)

(U) [Poaching Nets Discovered in the Chesapeake Bay off Tillman Island, MD, Pg. 4](#)

(U//FOUO) [Suspicious Activity at Blount Island Marine Terminal, Jacksonville, FL, Pg. 5](#)

(U//FOUO) [Security Breach at the SSA Marine Terminal, Long Beach, CA, Pg. 6](#)

(U//FOUO) [Illegal Panga Landing at Crystal Cove, Laguna Beach, CA, Pg. 7](#)

(U//FOUO) [Maritime Smuggling Event at Imperial Beach, CA, Pg. 8](#)

(U//FOUO) [Crewmember Deserted from the M/V NORWEGIAN PEARL, San Francisco, CA, Pg. 9](#)

(U//FOUO) [Abandoned Pleasure Craft Used in Smuggling Event in Ventura Cove Park, CA, Pg. 10](#)

^A (U) HOMEPORT is a publicly accessible Internet portal providing all users with current maritime security information. It is available on NIPRNET at: <https://homeport.uscg.mil/mycg/portal/cp/home.do>.

^B (U) Risk mitigation is a continuous process involving all stakeholders. This threat summary assumes that, if an adversary develops or transfers an attack capability against a target within the Sector, an attack could potentially occur with little or no time for law enforcement to detect, interdict, or disrupt the evolving plot. Therefore, it is incumbent on local port officials to continue their efforts to identify and address potential vulnerabilities, as well as actions to lessen disruptions, losses, or other attack consequences, regardless of the absence of a specific, tenable threat.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Figure 2.38 A Coast Guard Marine Threat Summary sample report.

(Continued)

2.5 DHS in the Age of President Donald J. Trump: 2016–2021

UNCLASSIFIED//FOR OFFICIAL USE ONLY

MARITIME HOMELAND THREAT ANALYSIS BRANCH MARITIME THREAT SUMMARY

1 JUN 2011 – ICC-HSEC-016-11

(U) INCIDENTS OF LAW ENFORCEMENT CONCERN

(U//FOUO) *GAO Investigators Used Fraudulent TWIC Cards to Access US Seaports*

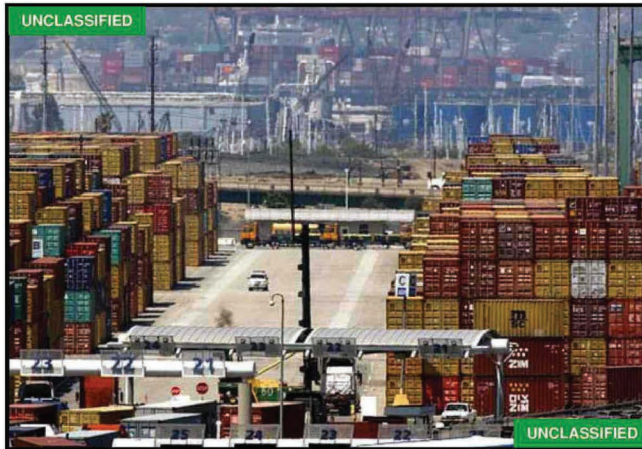


Figure 1: (U) Port of Los Angeles–Long Beach, Long Beach, CA.^c

(U//FOUO) According to a May 2011 report from the Government Accountability Office (GAO), undercover GAO investigators conducted security tests in 2009 at nine of the largest commercial ports in the United States which revealed serious security breaches. GAO investigators accessed the ports using counterfeit Transportation Worker Identification Credential (TWIC) cards, authentic cards acquired through fraudulent means, and by stating false reasons for needing facility access. Port security allowed undercover investigators, who posed as port personnel and drove vehicles containing simulated explosives, to enter secure port areas.

^c (U) Image of Port of Los Angeles–Long Beach: www.latimes.com/news/la-fi-port-smuggling-201110408.0.4299005.full.story

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Figure 2.38 (CONTINUED) A Coast Guard Marine Threat Summary sample report.

- **Division:** Flotillas in the same general geographic area are grouped into Divisions. The Division provides administrative, training, and supervisory support to Flotillas and promotes District and National policy.
- **Flotilla:** The Flotilla is the basic organizational unit of the Auxiliary and is comprised of at least 15 qualified members who carry out the day-to-day missions of “Team Coast Guard.” Every Auxiliary member is part of a Flotilla.

2.5.4.2 U.S. Secret Service

Given how threat and attack targets are often high-profile political figures, the decision to move the Secret Service under the roof of DHS is mission consistent.

The Secret Service is entrusted with the protection of the following figures:



Figure 2.39 Coast Guard Auxiliary logo.

- The president, the vice president (or other individuals next in order of succession to the Office of the President), the president-elect, and the vice president-elect.
- The immediate families of the above individuals.
- Former presidents and their spouses for their lifetimes, except when the spouse remarries. In 1997, congressional legislation became effective limiting Secret Service protection to former presidents for a period of not more than 10 years from the date the former president leaves office.
- Children of former presidents until age 16.
- Visiting heads of foreign states or governments and their spouses traveling with them, other distinguished foreign visitors to the United States, and official representatives of the United States performing special missions abroad.
- Major presidential and vice presidential candidates, and their spouses, within 120 days of a general presidential election.
- Other individuals as designated per executive order of the president.
- National Special Security Events, when designated as such by the secretary of DHS (Figure 2.40).

The overall goals of the Secret Service are graphically portrayed in the 2018–2022 Strategic Plan.



Figure 2.40 Pope Francis on his September 15, 2015 visit with Secret Service protection. (<http://www.secretservice.gov/press/gallery>.)

Goal 1 Strengthen the Integrated Mission

- Objective 1.1 Maintain excellence across integrated mission operations in physical and cyber space.
- Objective 1.2 Obtain, analyze, and share operational information
- Objective 1.3 Deploy tactical technologies that increase operational capabilities and address evolving threats

Goal 2 Grow and Support the Workforce

- Objective 2.1 Achieve optimal staffing levels through increased hiring and retention across the workforce
- Objective 2.2 Ensure personnel have access to and are able to attend relevant training opportunities
- Objective 2.3 Define and implement career progression pathways that are responsive to workforce and organizational needs
- Objective 2.4 Develop and promote processes and initiatives to improve morale and work-life balance

Goal 3 Identify, Develop, and Empower Leaders

- Objective 3.1 Formalize programs for leader identification and development at all levels across the workforce
- Objective 3.2 Increase standardization in promotion processes, factoring holistic feedback into performance evaluations
- Objective 3.3 Empower and increase accountability for enterprise-level decision-making at appropriate leadership levels

Goal 4 Modernize Business Processes

- Objective 4.1 Fully implement mission-based budgeting
- Objective 4.2 Execute efficient business processes and standardize proactive acquisition or up-to-date equipment
- Objective 4.3 Fully develop and employ a reliable, adaptive, and resilient information technology environment
- Objective 4.4 Increase use of robust analytical capabilities to make data-driven and risk-informed decisions

Goal 5 Increase Communications and Collaboration

- Objective 5.1 Strengthen internal communications pathways throughout the organization
- Objective 5.2 Increase collaboration opportunities across the workforce
- Objective 5.3 Expand traditional and innovative communication efforts to actively market the Secret Service brand
- Objective 5.4 Continue to leverage partnerships and increase outreach to enhance Service capabilities⁵⁸



Figure 2.41 Image of the higher fencing surrounding the White House.

For most of its history, the Secret Service has done an admirable job of protecting Presidents. Of recent history has been breaches in the White House fencing perimeter—no party more audacious than former Iraq military veteran, Omar Gonzalez.⁵⁹ See Figure 2.41 for a graphic of the new five-foot taller fence.

After scaling the fence, he actually made into the White House compound.⁶⁰ This was not Gonzalez's first encounter with security breaches along the perimeter at the White House.⁶¹ In addition, the events of January 6, 2021 and the storming of the capitol by Trump supporters has dramatically increased the focus and considerations for security measures in Washington DC.

Internet Exercise: Read the redacted Internal Report by the Secret Service on this character at: <https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-64-Apr16.pdf>

The Secret Service also deals with counterfeiting and select federal crimes not aligned to homeland security issues. Its investigations unit deals with identity crimes such as access device fraud, identity theft, false identification fraud, bank and check fraud, telemarketing fraud, telecommunications fraud (cellular and hard wire), computer fraud, fraud targeting automated payment systems and teller machines, direct deposit fraud, and investigations of forgery. For homeland purposes, the protection unit assumes a central role.

Two areas where the Secret Service orchestrates protective services are in major events and threat assessment. In the first instance, major events, the Secret Service coordinates agencies and their respective resources when a significant public event, involving protected persons, takes place. In this case, the secretary of DHS designates the event as a National Special Security Event (NSSE). The Secret Service assumes its mandated role as the lead agency for the design and implementation of the operational security plan. The NSSE is coordinated in cooperation with its established partnerships with law enforcement and public safety officials at the local, state, and federal levels.

A second integral contribution of the service is the development and operational oversight of the National Threat Assessment Center. The Center focuses its research and activities on the protection of public figures, the creation and implementation of best practices in the protection thereof, and recommendations on how best to serve potential targets of threat. The Center directs its attention chiefly to:

- Research on threat assessment and various types of targeted violence
- Training on threat assessment and targeted violence to law enforcement officials and others with protective and public safety responsibilities
- Information sharing among agencies with protective or public safety responsibilities
- Programs to promote the standardization of federal, state, and local threat assessment and investigations involving threats

2.5 DHS in the Age of President Donald J. Trump: 2016–2021

Internet Exercise: While the Secret Service generally has had an impeccable and unassailable reputation, certain allegations emerged regarding improper behavior in Cartagena, Colombia, in 2013 and other failures to protect the White House perimeter in 2014–2015. The reports by the inspector general (IG) regarding these investigations are heavily redacted. See the Office of the Inspector General (OIG) website at <http://www.oig.dhs.gov>; click on the Freedom of Information Act (FOIA) Reading Room link and review the records concerning the U.S. Secret Service.

2.5.4.3 Federal Law Enforcement Training Center

Just as it was wise to relocate the USCG and the Secret Service to DHS, it makes eminent sense to move the federal government's premier training agency under the same roof (Figure 2.42).

FLETC has assumed a central role in the training of law enforcement professionals across the United States. From every jurisdiction, justice professionals benefit from expertise and cutting-edge subject matter relevant to homeland security (Figure 2.43).



Figure 2.42 Federal Law Enforcement Training Center in Glynn County, Georgia. (National Parks Service website at www.nps.gov.)



Figure 2.43 On any given day, there are roughly 7,000 personnel at the Federal Law Enforcement Training Centers (FLETC) facilities across the nation. (From Department of Homeland Security.)

Homeland Security

FLETC is located in Glynnco, Georgia, with satellite facilities in Washington, DC; Jacksonville, Florida; Charleston, South Carolina; Artesia, New Mexico; and Cheltenham, Maryland. The strategic goals of FLETC are to

- Provide training that enables our partners to accomplish their missions
- Foster a high-performing workforce
- Provide mission-responsive infrastructure
- Optimize business practices

See Figure 2.44 for an organization chart of the FLETC hierarchy.

Each facility provides a wide array of training opportunities. Those more appropriately applicable to homeland security are:

- Antiterrorism Intelligence Awareness Training Program (AIATP)
- Commercial Vehicle Counterterrorism Training Program (CVCTP)
- Computer Network Investigations Training Program (CNITP)
- Covert Electronic Surveillance Program (CESP)
- Covert Electronic Tracking Program (CETP)
- Crisis Management Training Program (CMTTP)
- Critical Incident Response Training Program (CIRTP)
- Critical Infrastructure Key Resource Protection Qualification Training Program (CIKRTP)
- Critical Infrastructure Protection Training Program (CIPTP)
- Cyber Counterterrorism Investigations Training Program (CCITP)
- Domestic Terrorism and Hate Crimes Training Program (DTHCTP)
- Intelligence Analyst Training Program (IATP)
- Intelligence Awareness for Law Enforcement Executives Training Program (IALEETP)
- International Banking and Money Laundering Training Program (IBMLTP)
- Internet Investigations Training Program (IITP)
- Internet Protocol Camera Program (IPCP)
- Introductory Intelligence Analyst Training Program (IIATP)
- Operations Security for Public Safety Agencies Counterterrorism Training Program (OPSACTP)
- Seaport Security Antiterrorism Training Program (SSATP)
- Suicide Bomber Mitigation Training Program (SBMTP)
- Vehicle Ambush Countermeasures Training Program (VACTP)
- Weapons of Mass Destruction Training Program (Level I) (WMDTP L1—Operations—Core NFPA 472.5)
- Weapons of Mass Destruction Training Program (Level II) (WMDTP L2—Technician)

FLETC dedicates a large portion of its training to terrorism and counterterrorism. An entire certification program exists for those seeking this specialized knowledge. FLETC delivers state-of-the-art training in advanced topics relevant to homeland security, including

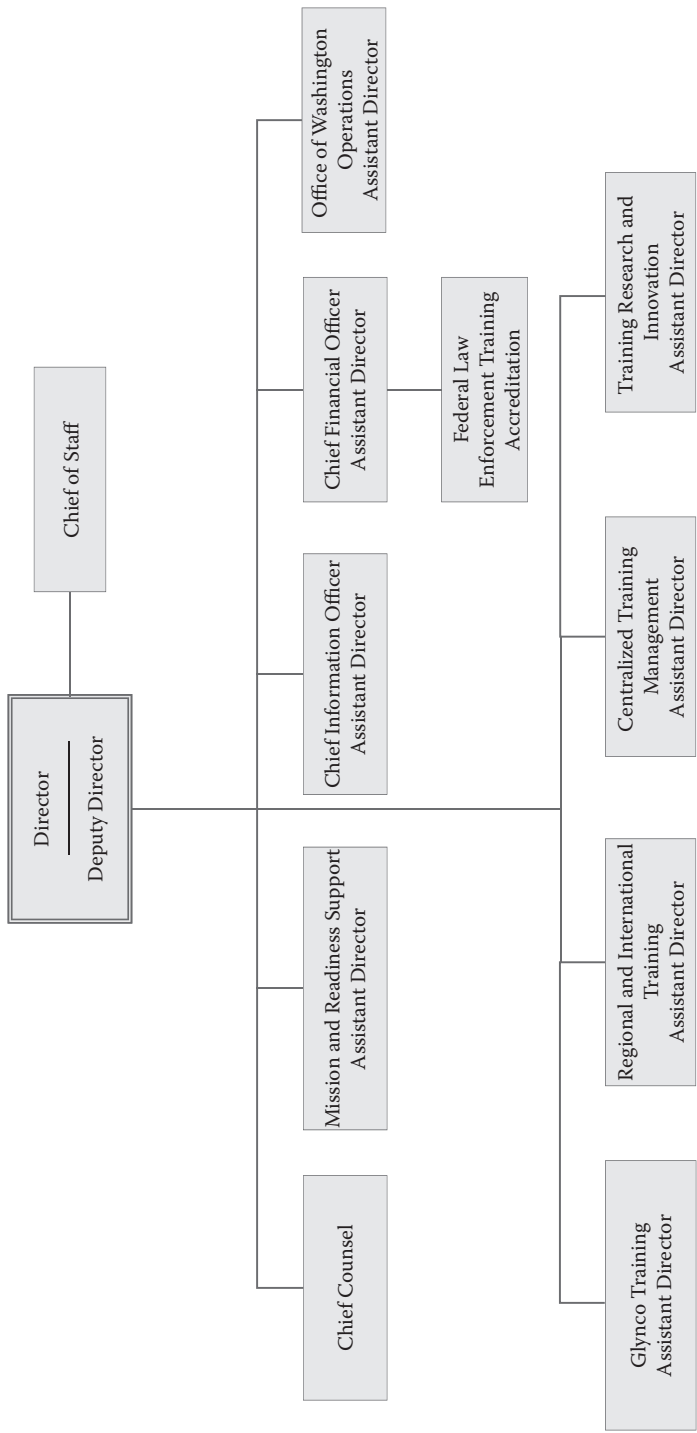


Figure 2.44 Federal Law Enforcement Training Center hierarchy, July 12, 2015. (<http://www.fletc.gov/fletc-organization-chart-ppt>.)

Homeland Security

- Cyber-terrorism training
- Critical infrastructure training
- Antiterrorism intelligence

Internet Exercise: For a full catalog of courses, see <https://www.fletc.gov/training-catalog>

2.5.5 Advisory Panels and Committees

One of the recurring themes in DHS operations is the agency's willingness to work with external authority—both public and private. The council is more than a mere formality but an essential contributor to the integrity of the homeland effort. So integral is the council considered to the mission of DHS that the body is statutorily required to report its recommendations every 4 years. Reports from May 27, 2010, urge the agency to “define and operationalize the strategic framework; to delineate roles and responsibilities” with a keener eye and to measure DHS mission with “measurable outcomes...and targets to drive alignment of the Department’s priorities, structures, systems and resources.”⁶²

That operational outlook was further confirmed in the IG's management and performance review of the agency in February 2015. This report, as well as other recent studies, urges DHS to be far more efficient in resources, to keep open to external partnerships, and to take the needed steps to ensure a safe border.⁶³ The DHS has largely adopted the recommendations relative to strategic planning. The level of strategic planning will depend on the subject matter and the priority of interests, as previously outlined in Figure 2.23.⁶⁴

The strategic approach is quite evident in the DHS 2018–2020 annual performance review, the department reiterated its primary performance measures.⁶⁵ DHS centers its attention on the areas of performance shown in Figure 2.45.⁶⁶



Figure 2.45 Diagram from a DHS Annual Performance Report.

These reports serve as a critique of DHS using the combined wisdom of the committee as outside, objective observers. The aim is for the council to turn a critical and pragmatic eye on DHS programs and offer recommendations for improvement and to curtail initiatives that may be redundant or not properly vetted, to avoid unnecessary bureaucracy within the department.

The council wisely calls for the aggressive integration and melding of state and local governmental authorities, working side by side with federal entities in law enforcement and the intelligence community; the agency also seeks input and professional participation by other suitable means. One avenue erects and establishes a body of government leaders, scholars, and practitioners that give advice to DHS. DHS labels these groups as subcommittees, task forces, and panels.⁶⁷

Some of the more prominent panels are:

- Economic Security Subcommittee
- Information and Communications Technology Risk Reduction Subcommittee
- Youth Engagement Subcommittee
- Biometrics Subcommittee
- Prevention of Targeted Violence Against Faith-Based Communities Subcommittee
- State, Local, Tribal, and Territorial Cyber Security Subcommittee
- CBP Families and Children Care Panel Subcommittee
- Countering Foreign Influence Subcommittee
- Emerging Technologies Subcommittee⁶⁸

Current members of the Homeland Security Advisory Council are as follows:

- William Webster (Chair), Retired Partner, Milbank, Tweed, Hadley & McCloy, LLP
- William Bratton (Vice Chair), Executive Chairman, Teneo Risk
- Karen Tandy, Administrator (Ret.), Drug Enforcement Administration

For the charter that established the HSAC, see Appendix A.

DHS also relies on specialized committees that deal with topics of significant interest to the agency. Presently, these committees are designated as senior advisory committees, an example referenced later in this chapter.

Other areas of expertise are solicited in private sector justice, secure borders, state and local officials, and the academe. These committees issue reports and recommendations to the secretary as needed.

Internet Exercise: For an example of a committee report dealing with secure borders, visit http://www.dhs.gov/xlibrary/assets/hsac_SBODACreport508-compliant_version2.pdf.

Since 2011, under the leadership of President Barack Obama, the Advisory Council had been asked to erect a Task Force on Secure Communities. The initiative gives special attention to the problem of illegal immigration and how it impacts community safety.

Internet Exercise: Visit the task force's draft recommendations on how to secure border towns directly suffering from the problems and challenges of illegal immigration at <http://www.dhs.gov/xlibrary/assets/hsac-task-force-on-secure-communities.pdf>.

2.6 Conclusion

Chapter 2 began with a review of the events of September 11, 2001, as well subsequent examples of this nation's perpetual challenge against threats coupled with a discussion of the immediate responses of governmental agencies. The lack of coordination, cooperation, and information

Homeland Security

sharing between federal agencies was discussed as a contributing factor to the attacks. The strategies and tactics developed as a result, namely, the creation of DHS and its many directorates and committees, were next introduced.

DHS was created to be a flexible entity, one that can change to reflect national security needs at any given time. This is apparent in the fluctuation in the organization's structure in its first 8 years of existence. The text next turned to the initial formation of the department from 2001 to 2003, its strategic goals and mission, and its initial policy formulation. The *Homeland Security Act of 2002* established the department itself and outlined its powers, main areas of responsibility, and authority. Its early evolution and early department mergers were presented. Nearly 20 years later, DHS retains many of its original structural features but has evolved and transformed itself repeatedly.

As with any bureaucratic entity, change is inevitable, and this was never more apparent than in the major reorganization of DHS between 2003 and 2008. The text next highlighted the first four secretaries of DHS and the agency's various directorates and offices and their corresponding responsibilities. During this major reorganization phase, many government agencies were swept under DHS's mantle and partially or, in some cases, completely reorganized. The four major agency reorganizations, including the USCG, the Secret Service, FPS, and FLETC, were analyzed in depth. FPS's move to the Management Directorate was highlighted, and the crucial role of CISA, which subsumed the former National Planning and Preparedness Directorate (NPPD), was fully covered. Finally, DHS's advisory panel and committee structure were explained.

Keywords

Agency Culture; Border Security; Bureaucracy; Central Intelligence Agency; CISA; Coast Guard; Counterterrorism; Critical Infrastructure; Customs and Border Protection; Department of Homeland Security; Directorate; Domestic Nuclear Detection Office; Drug Enforcement Administration; Emergency Management; Federal Aviation Administration; Federal Bureau of Investigation; Federal Emergency Management Agency; FLETC; Hijack; Homeland Security Act of 2002; Illegal Aliens; Immigration and Customs Enforcement; Infrastructure; Intelligence; Intelligence Sharing; Interagency Cooperation; Law Enforcement; Maritime Security; Mitigation; National Commission on 9/11; National Defense; National Security Agency; National Threat Assessment Center; Natural Disaster; NORAD; Pentagon; Prevention; Protective Services; Public Safety; Secret Service; Security Survey; Targeted Violence; Threat Analysis; Threat Assessment; Transportation Security Administration; U.S. Citizenship and Immigration Services; Vulnerability Assessment; Weapons of Mass Destruction;

Discussion Questions

1. How would you rate the federal government response to 9/11 as compared with more recent disasters such as Hurricane Katrina and Hurricane Sandy?
2. Why did an agency for homeland security evolve?
3. What alternatives to DHS are possible?
4. What is the most striking difference between DHS 2003 and DHS today?
5. Does DHS have a political edge? Does DHS reflect who is in power?
6. Which agencies might be arguably misplaced in DHS?
7. How do lay people and lay organizations impact DHS?

Practical Exercises

1. Visit DHS's website and access the pages regarding the three directorates. List the programs and offices that each directorate supervises.
2. Review the list of agencies that were swept into DHS during the reorganization. Can you think of a better plan or reorganization? Does the current organization make sense from an operational perspective?
3. Visit the USCG website. Find out about maritime security (MARSEC) levels.
4. Visit the U.S. Secret Service's website and locate information on the National Threat Assessment Center. Find out about their current major research projects.
5. Visit the FPS section of the ICE website. Locate current job vacancies and familiarize yourself with the requirements for hire by the FPS.

Notes

- 1 Federal Bureau of Investigation, Famous cases and criminals, 9/11 Investigation (PENTTBOM), <https://www.fbi.gov/history/famous-cases/911-investigation> (accessed August 8, 2020).
- 2 See: A. Durkee, "AOC Goes to the Border, Shares the 'Systemic Cruelty' of Migrant Detention Centers," *Vanity Fair*, July 2, 2019, <https://www.vanityfair.com/news/2019/07/aoc-ocasio-cortez-congress-migrant-detention-centers> (accessed August 8, 2020).
- 3 V. Morton, "Rep. Ilhan Omar calls for elimination of Customs and Border Protection, other 'rogue agencies'," *The Washington Times*, July 3, 2019, <https://www.washingtontimes.com/news/2019/jul/3/ilhan-omar-calls-elimination-customs-and-border-pr/> (accessed August 8, 2020).
- 4 See: US Department of Homeland Security, Press Release December 12, 2018, "Walls Work," <https://www.dhs.gov/news/2018/12/12/walls-work> (accessed August 8, 2020).
- 5 See: C. Felter, D. Renwick and A. Cheatham, "The US Immigration Debate," UC Council on Foreign Relations, June 23, 2020, <https://www.cfr.org/backgrounder/us-immigration-debate-0> (accessed August 8, 2020).
- 6 FOXNews.com, News Archive, Timeline: September 11, 2001, <https://www.foxnews.com/story/timeline-sept-11-2001> (accessed August 8, 2020).
- 7 For an interesting look into the cultural shifts in the intelligence community as it evaluated terrorism, see T. A. Gilly, *Deconstructing terrorism: Counter-terrorism's trajectory for the 21st century*, *The Homeland Security Review*, 5 (2011): 5.
- 8 National Commission on Terrorist Attacks upon the United States, Tenth Public Hearing, Law Enforcement, Counterterrorism, and Intelligence Collection in the United States prior to 9/11, Staff Statement No. 9, April 13, 2004, 8, http://govinfo.library.unt.edu/911/staff_statements/staff_statement_9.pdf (accessed August 8, 2020).
- 9 R. Ward et al., *Homeland Security: An Introduction* (Cincinnati, OH: Anderson Publishing Co., 2006), 57.
- 10 See: L. M. Segarra, "FBI Admits It Failed to Investigate Tip About Accused Florida School Shooter in January," *Time*, February 17, 2018, Originally Published February 16, 2018, <https://time.com/5162999/fbi-failed-investigate-tip-nikolas-cruz/> (accessed August 8, 2020).
- 11 See: M. Rubio, US Senator, Website, "Press Release: Rubio: FBI Utterly Failed Victims of Florida Shooting," February 16, 2018, <https://www.rubio.senate.gov/public/index.cfm/press-releases?ID=9BCDA794-40A9-443B-A6A2-9B772A823F8B> (accessed August 8, 2020).
- 12 See: A. Pressman, "The Secret History of the FBI's Battle Against Apple Reveals the Bureau's Mistakes," *Fortune.com*, March 27, 2018, <https://fortune.com/2018/03/27/fbi-apple-iphone-encryption-san-bernardino/> (accessed August 8, 2020).
- 13 Bullock, *Homeland Security*, 23.
- 14 President G. W. Bush, *The Department of Homeland Security* (Washington, DC: U.S. Government Printing Office, June 19–23, 2002), <http://www.dhs.gov/xlibrary/assets/book.pdf> (accessed August 8, 2020).

Homeland Security

- 15 Bush, *Department Homeland Security*, 1, <http://www.dhs.gov/xlibrary/assets/book.pdf> (accessed August 8, 2020).
- 16 Ibid.
- 17 *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, Official Government Edition (Washington, DC: U.S. Government Printing Office, July 22, 2004), 400.
- 18 Homeland Security Council, National Strategy for Homeland Security (October 2007), 3, <https://www.dhs.gov/national-strategy-homeland-security-october-2007> (accessed August 8, 2020).
- 19 Homeland Security Act of 2002, U.S. Code 6 (2002), section 101.
- 20 Ibid, section 101 (b).
- 21 S. S. Gressle, CRS Report for Congress, Department of Homeland Security Organization Chart, Order Code RS21366 (January 14, 2004), <https://www.hsdl.org/?view&did=451595> (accessed August 8, 2020).
- 22 Homeland Security Act of 2002, U.S. Code 6 (2002), section 1502.
- 23 Office of Homeland Security, The National Strategy for Homeland Security (June 16, 2002), vii, http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accessed August 8, 2020).
- 24 The Federal News Radio reports that support for consolidation is growing in the U.S. Senate, <http://www.federalnewsradio.com/?nid=108&sid=2545915> (accessed August 8, 2020).
- 25 US Department of Homeland Security Organizational Chart, https://www.dhs.gov/sites/default/files/publications/19_1205_dhs-organizational-chart.pdf (accessed August 8, 2020).
- 26 See B. Forer, TSA Full-Body Scanners: No More Naked Images, ABCnews.com, July 21, 2011, <http://abcnews.go.com/Travel/Travel/tsa-full-body-scanners-naked-images/story?id=14125474> (accessed August 8, 2020).
- 27 See: J. Johnson, “Stop the political blame game, so we can solve our crisis first,” *The Hill*, March 28, 2020, <https://thehill.com/opinion/white-house/490024-jeh-johnson-stop-the-political-blame-game-so-we-can-solve-our-crisis> (accessed August 8, 2020).
- 28 See: T. Hains, “Obama DHS Sec. Jeh Johnson: I Freely Admit We Detained Children, “It Was Necessary,”” *RealClear Politics*, June 24, 2018, https://www.realclearpolitics.com/video/2018/06/24/obama_dhs_sec_jeh_johnson_we_detained_children_it_was_necessary.html (accessed August 8, 2020).
- 29 J. C. Johnson, *Memorandum on Policies for the Apprehension, Detention and Removal of Undocumented Immigrants* (November 20, 2014), https://www.dhs.gov/sites/default/files/publications/14_1120_memo_prosecutorial_discretion.pdf (accessed August 8, 2020).
- 30 C. Carcamo, U.S. policy change may enable speedy release of detained immigrant families, *LA Times Online* (June 24, 2015), <http://www.latimes.com/nation/la-na-immigration-family-detention-20150624-story.html> (accessed August 8, 2020).
- 31 Statement by Secretary Jeh C. Johnson on DHS’s New Office for Community Partnerships (September 28, 2015), <https://www.dhs.gov/news/2015/09/28/statement-secretary-jeh-c-johnson-dhs%E2%80%99s-new-office-community-partnerships> (accessed August 8, 2020).
- 32 See: A. R. Arthur, “Trump Win in Decision on Family Separations: Judge rules government is not ‘systematically separating families at the border’,” Center for Immigration Studies, January 15, 2020, <https://cis.org/Arthur/Trump-Win-Decision-Family-Separations> (accessed August 8, 2020).
- 33 For the storyline on Secretary Nielsen, see: “Kirstjen Nielsen steps down as secretary of homeland security,” *The Economist*, April 8, 2019, <https://www.economist.com/democracy-in-america/2019/04/08/kirstjen-nielsen-steps-down-as-secretary-of-homeland-security> (accessed August 8, 2020).
- 34 US Department of Homeland Security, “Fact Sheet: DHS Strategic Framework for Countering Terrorism and Targeted Violence,” https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-ct-tv-fact-sheet.pdf (accessed August 8, 2020).
- 35 Ibid.
- 36 See: “Kevin McAleenan: US Homeland Security chief steps down,” *BBC News*, October 12, 2019, <https://www.bbc.com/news/world-us-canada-50023448> (accessed August 8, 2020).
- 37 US Department of Homeland Security, Strategic Framework for Countering Terrorism and Targeted Violence 31 (September 2019), https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf (accessed August 8, 2020).
- 38 For the full text of the plan, see Ibid.
- 39 Cybersecurity & Infrastructure Security Agency webpage, <https://www.cisa.gov/> (accessed August 8, 2020).

- 40 Cybersecurity & Infrastructure Security Agency, Identifying Critical Infrastructure During COVID-19 webpage, <https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19> (accessed August 8, 2020).
- 41 See: NCCIC Year in Review 2017, Operation Cyber Guardian, https://www.us-cert.gov/sites/default/files/publications/NCCIC_Year_in_Review_2017_Final.pdf (accessed August 8, 2020).
- 42 See: CISA, Cyber Storm VI: National Cyber Exercise Webpage, <https://www.cisa.gov/cyber-storm-vi> (accessed August 8, 2020).
- 43 CISA, National Risk Management Website, <https://www.cisa.gov/national-risk-management> (accessed August 8, 2020).
- 44 US Department of Homeland Security, Science & Technology Directorate, Under Secretary for S&T Organization Chart, https://www.dhs.gov/sites/default/files/publications/Organizational_Chart_External_10-01-18.pdf (accessed August 8, 2020).
- 45 For the White House and CDC recent guidelines on “Opening Up America” see: Opening Up America Again, https://www.whitehouse.gov/openingamerica/?utm_source=sandt_slideshow&utm_medium=web&utm_campaign=dhsgov (accessed August 8, 2020).
- 46 US Department of Homeland Security, Directorate of Science and Technology, <https://www.dhs.gov/science-and-technology/about-st> (accessed August 8, 2020).
- 47 US Department of Homeland Security, Management Directorate Organization Chart, <https://www.dhs.gov/sites/default/files/publications/MGMT%20Org%20Chart%202018.12.18.pdf> (accessed August 8, 2020).
- 48 In its earlier life, DHS tended to specialize in singular topics rather than merge them. Read this interesting GAO observation of how the scattered approach evolved into a more unified delivery at: US Government Accountability Office, “Homeland Security: DHS’s Chemical, Biological, Radiological, and Nuclear Program Consolidation Efforts,” December 7, 2017, <https://www.gao.gov/products/GAO-18-284T> (accessed August 8, 2020).
- 49 US Department of Homeland Security Website, Operational and Support Components Webpage, <https://www.dhs.gov/operational-and-support-components> (accessed August 8, 2020).
- 50 See: Captain G. J. Sanial, “The Coast Guard Belongs with DoD,” US Naval Institute Proceedings, September 2019, <https://www.usni.org/magazines/proceedings/2019/september/coast-guard-belongs-dod> (accessed August 8, 2020).
- 51 United States Coast Guard, “Missions,” <https://www.history.uscg.mil/home/Missions/> (accessed August 8, 2020).
- 52 United States Coast Guard, <http://www.uscg.mil> (accessed August 8, 2020).
- 53 USCG Intelligence Coordination Center, Maritime Threat Summary, <https://info.publicintelligence.net/USCG-MaritimeThreats.pdf> (accessed August 8, 2020).
- 54 V. Crea, The U.S. Coast Guard: A flexible force for national security, *Naval War College Review*, 60 (Winter 2007): 15–23; See also how the Coast Guard Fleet is rational deployed in: Department of the Navy, The National Fleet Plan, August 2015, <https://info.publicintelligence.net/USNavy-FleetPlan-2015.pdf> (accessed August 8, 2020).
- 55 T. Allen, New threats, new challenges: The coast guard’s new strategy, *Proceedings*, 133 (March 2007): 74.
- 56 B. B. Stubbs, U.S. coast guard annual review, *Proceedings*, 133 (May 2007): 84.
- 57 Stubbs, *Proceedings*, 84; see also *The US Coast Guard of the 21st Century*, <https://media.defense.gov/2017/Jun/26/2001769014/-1/-1/0/21STCENTURY.PDF> (accessed August 8, 2020).
- 58 US Secret Service, FY 2018-2022 Strategic Plan, 9 (May 2018), https://www.secretservice.gov/data/press/reports/USSS_FY18-22_Strategic_Plan.pdf (accessed August 8, 2020).
- 59 C. Schilling, “White House fence-jumper: Another victim of ‘psych crisis’ at Fort Hood?” WND, September 22, 2014, <https://www.wnd.com/2014/09/key-fact-about-white-house-fence-jumper-revealed/> (accessed August 8, 2020).
- 60 For an after-action report on this breach, see: US Secret Service, “Executive Summary to Report from the USSS Protective Mission Panel,” <https://www.scribd.com/document/250503128/Executive-Summary-to-Report-from-the-USSS-Protective-Mission-Panel> (accessed August 8, 2020).
- 61 US Dept. of Homeland Security, Office of the Inspector General, “2014 White House Fence Jumping Incident,” April 2016, <https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-64-Apr16.pdf> (accessed August 8, 2020).

Homeland Security

- 62 Department of Homeland Security, Homeland Security Advisory Council, Quadrennial Review Advisory Committee: Final Report 8–9, May 27, 2010.
- 63 Office of the Inspector General, *Major Management and Performance Challenges Facing the Department of Homeland Security* (Revised), February 23, 2015, https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-09_Feb15.pdf (accessed August 8, 2020).
- 64 US Department of Homeland Security, Strategic Framework for Countering Terrorism and Targeted Violence 31 (September 2019), https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf (accessed August 8, 2020).
- 65 See: US Department of Homeland Security, “FY 2018–2020 Annual Performance Report,” https://www.dhs.gov/sites/default/files/publications/19_0318_MGMT_CBJ-Annual-Performance-Review-DHS-Overview_0.pdf (accessed August 8, 2020).
- 66 Ibid.; Office of the Inspector General, *Major Management and Performance Challenges Facing the Department of Homeland Security* (Revised), 1 (February 23, 2015), https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-09_Feb15.pdf (accessed August 8, 2020).
- 67 The subcommittees often issue reports and recommendations to the DHS. An example is at: US Dept of Homeland Security Website, Emerging Technologies Subcommittee page, <https://www.dhs.gov/publication/emerging-technologies-subcommittee> (accessed August 8, 2020).
- 68 US Dept of Homeland Security Website, Homeland Security Advisory Council page, <https://www.dhs.gov/homeland-security-advisory-council> (accessed August 8, 2020).

3

Homeland Security Law, Regulations, and Budgeting

OBJECTIVES

1. To identify the major laws, regulations, and executive orders that form and govern the Department of Homeland Security (DHS)
2. To analyze Executive Order 13228, which created DHS; and Executive Order 13231, which focuses on the national infrastructure and its protection
3. To summarize the provisions of the Homeland Security Act of 2002
4. To describe the USA Patriot Act, its provisions, and its authority
5. To comprehend the various specialized laws that govern certain operations within DHS, such as the REAL ID program, Office of Biometric Identity Management, the SAFETY Act, and the like
6. To explain the reasoning behind budgeting priorities in DHS and why the priorities fluctuate from year to year
7. To compare the changes in allotments and priorities in DHS budgets from the agency's inception to the present
8. To predict where future allotments in DHS budgets may change and why

3.1 Introduction

Exactly how the affairs of DHS are managed is an ongoing and very vibrant topic. The power of DHS emanates from the legal authority that initiated its existence. Laws, regulations, and executive orders enable the agency to carry out its aim and purpose. Many laws touch on the functions of homeland defense, such as in matters of privacy, arrest, search, and wiretap, while other laws establish centers of research, operational funds for new initiatives, or primers for a new directive. Funding for DHS is just as important. Without money, the agency would have no life whatsoever. How Congress and the president eventually agree to fund DHS is an annual

Homeland Security

responsibility. From another management perspective, DHS needs to evaluate how it interacts with other governmental authorities—namely, state and local entities; this is a perpetual policy concern and consideration for DHS. If anything is certain, it is that DHS needs to collaborate at every governmental level. Just as importantly, DHS will need to work closely and cooperatively with private-sector justice as well, since private-sector justice is the country's fastest-growing arm in the criminal justice body. Privatization is a reality that must be factored in as DHS manages its affairs.

3.2 Homeland Security Law, Regulations, and Executive Orders

The power of DHS is derived from its legal authority. Soon after the September 11, 2001, attacks, President George W. Bush sought to establish an agency dedicated to the protection of the homeland. The speed with which these promulgations occurred not only impressed but also manifested the urgency of these tragic events.

3.2.1 Executive Order 13228: Origin of DHS

By executive order dated October 11, 2001, the president calls for the establishment of DHS, lays out its mission, categorizes its purpose and aim, and sets an early tone for how this agency will develop (see Figure 3.1).

3.2.2 Executive Order 13231: Protection of Infrastructure

Shortly thereafter, President Bush issued another executive order that focused on the nation's infrastructure. Given the recent events, the president, as well as Congress, was rightfully concerned about the country's infrastructure of transportation, water, energy and power plants, and other essential components of the American way of life. At the time, there were serious, very legitimate concerns about these facilities. Executive Order 13231 (Figure 3.2), signed October 16, 2001, dealt directly with infrastructure.

Internet Exercise: For final administrative rules on the protection of infrastructure, see https://www.dhs.gov/sites/default/files/publications/pcii_final_rule_federal_register9-1-06-2_508.pdf.

The executive branch's view of infrastructure had been heightened over the term of President Barack Obama. In matters of funding and operational priorities, President Obama had repeatedly emphasized the interconnectedness of our infrastructure assets and urged agencies to prioritize the protection of our infrastructure in a more holistic way. By Presidential Proclamation 8607, President Obama declared that December 2010 was "Critical Infrastructure Protection Month" and noted that infrastructure is "essential to the security, economic welfare, public health and safety of the United States."¹ In 2012, the proclamation was renamed "Critical Infrastructure and Resilience Month."² A year later, President Obama continued his rightful emphasis on the protection of infrastructure by adding a "cybersecurity" dimension to previous decrees³ (see Figure 3.3).

3.2.3 Executive Order 13223: September 14, 2001

Aligned with the establishment of the DHS and its various powers, other Executive Orders dealt with the power of the Presidency to administer said agency and in the case of 13223 to integrate and utilize military and defense functions in time of national emergency. The Order states in part:

Executive Order 13223 of September 14, 2001 Ordering the Ready Reserve of the Armed Forces To Active Duty and Delegating Certain Authorities to the Secretary of Defense and the Secretary of Transportation By the authority vested in me as President by the Constitution and the laws of

3.2 Homeland Security Law, Regulations, and Executive Orders

EXECUTIVE ORDER: ESTABLISHING THE OFFICE OF HOMELAND SECURITY AND THE HOMELAND SECURITY COUNCIL

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Establishment. I hereby establish within the Executive Office of the President an Office of Homeland Security (the "Office") to be headed by the Assistant to the President for Homeland Security.

Sec. 2. Mission. The mission of the Office shall be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. The Office shall perform the functions necessary to carry out this mission, including the functions specified in section 3 of this order.

Sec. 3. Functions. The functions of the Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States.

- (a) National Strategy. The Office shall work with executive departments and agencies, State and local governments, and private entities to ensure the adequacy of the national strategy for detecting, preparing for, preventing, protecting against, responding to, and recovering from terrorist threats or attacks within the United States and shall periodically review and coordinate revisions to that strategy as necessary.
- (b) Detection. The Office shall identify priorities and coordinate efforts for collection and analysis of information within the United States regarding threats of terrorism against the United States and activities of terrorists or terrorist groups within the United States. The Office also shall identify, in coordination with the Assistant to the President for National Security Affairs, priorities for collection of intelligence outside the United States regarding threats of terrorism within the United States.
 - (i) In performing these functions, the Office shall work with Federal, State, and local agencies, as appropriate, to:
 - (A) facilitate collection from State and local governments and private entities of information pertaining to terrorist threats or activities within the United States;
 - (B) coordinate and prioritize the requirements for foreign intelligence relating to terrorism within the United States of executive departments and agencies responsible for homeland security and provide these requirements and priorities to the Director of Central Intelligence and other agencies responsible collection of foreign intelligence;
 - (C) coordinate efforts to ensure that all executive departments and agencies that have intelligence collection responsibilities have sufficient technological capabilities and resources to collect intelligence and data relating to terrorist activities or possible terrorist acts within the United States, working with the Assistant to the President for National Security Affairs, as appropriate;
 - (D) coordinate development of monitoring protocols and equipment for use in detecting the release of biological, chemical, and radiological hazards; and
 - (E) ensure that, to the extent permitted by law, all appropriate and necessary intelligence and law enforcement information relating to homeland security is disseminated to and exchanged among appropriate executive departments and agencies responsible for homeland security and, where appropriate for reasons of homeland security, promote exchange of such information with and among State and local governments and private entities.
 - (ii) Executive departments and agencies shall, to the extent permitted by law, make available to the Office all information relating to terrorist threats and activities within the United States.
- (c) Preparedness. The Office of Homeland Security shall coordinate national efforts to prepare for and mitigate the consequences of terrorist threats or attacks within the United States. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate, to:
 - (i) review and assess the adequacy of the portions of all Federal emergency response plans that pertain to terrorist threats or attacks within the United States;
 - (ii) coordinate domestic exercises and simulations designed to assess and practice systems that would be called upon to respond to a terrorist threat or attack within the United States and coordinate programs and activities for training Federal, State, and local employees who would be called upon to respond to such a threat or attack;
 - (iii) coordinate national efforts to ensure public health preparedness for a terrorist attack, including reviewing vaccination policies and reviewing the adequacy of and, if necessary, increasing vaccine and pharmaceutical stockpiles and hospital capacity;
 - (iv) coordinate Federal assistance to State and local authorities and nongovernmental organizations to prepare for and respond to terrorist threats or attacks within the United States;

Figure 3.1 Executive order establishing the Department of Homeland Security.

(Continued)

Homeland Security

- (v) ensure that national preparedness programs and activities for terrorist threats or attacks are developed and are regularly evaluated under appropriate standards and that resources are allocated to improving and sustaining preparedness based on such evaluations; and
- (vi) ensure the readiness and coordinated deployment of Federal response teams to respond to terrorist threats or attacks, working with the Assistant to the President for National Security Affairs, when appropriate.
- (d) Prevention. The Office shall coordinate efforts to prevent terrorist attacks within the United States. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate, to:
 - (i) facilitate the exchange of information among such agencies relating to immigration and visa matters and shipments of cargo; and, working with the Assistant to the President for National Security Affairs, ensure coordination among such agencies to prevent the entry of terrorists and terrorist materials and supplies into the United States and facilitate removal of such terrorists from the United States, when appropriate;
 - (ii) coordinate efforts to investigate terrorist threats and attacks within the United States; and
 - (iii) coordinate efforts to improve the security of United States borders, territorial waters, and airspace in order to prevent acts of terrorism within the United States, working with the Assistant to the President for National Security Affairs, when appropriate.
- (e) Protection. The Office shall coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate, to:
 - (i) strengthen measures for protecting energy production, transmission, and distribution services and critical facilities; other utilities; telecommunications; facilities that produce, use, store, or dispose of nuclear material; and other critical infrastructure services and critical facilities within the United States from terrorist attack;
 - (ii) coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack;
 - (iii) develop criteria for reviewing whether appropriate security measures are in place at major public and privately owned facilities within the United States;
 - (iv) coordinate domestic efforts to ensure that special events determined by appropriate senior officials to have national significance are protected from terrorist attack;
 - (v) coordinate efforts to protect transportation systems within the United States, including railways, highways, shipping, ports and waterways, and airports and civilian aircraft, from terrorist attack;
 - (vi) coordinate efforts to protect United States livestock, agriculture, and systems for the provision of water and food for human use and consumption from terrorist attack; and
 - (vii) coordinate efforts to prevent unauthorized access to, development of, and unlawful importation into the United States of, chemical, biological, radiological, nuclear, explosive, or other related materials that have the potential to be used in terrorist attacks.
- (f) Response and Recovery. The Office shall coordinate efforts to respond to and promote recovery from terrorist threats or attacks within the United States. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate, to:
 - (i) coordinate efforts to ensure rapid restoration of transportation systems, energy production, transmission, and distribution systems; telecommunications; other utilities; and other critical infrastructure facilities after disruption by a terrorist threat or attack;
 - (ii) coordinate efforts to ensure rapid restoration of public and private critical information systems after disruption by a terrorist threat or attack;
 - (iii) work with the National Economic Council to coordinate efforts to stabilize United States financial markets after a terrorist threat or attack and manage the immediate economic and financial consequences of the incident;
 - (iv) coordinate Federal plans and programs to provide medical, financial, and other assistance to victims of terrorist attacks and their families; and
 - (v) coordinate containment and removal of biological, chemical, radiological, explosive, or other hazardous materials in the event of a terrorist threat or attack involving such hazards and coordinate efforts to mitigate the effects of such an attack.
- (g) Incident Management. The Assistant to the President for Homeland Security shall be the individual primarily responsible for coordinating the domestic response efforts of all departments and agencies in the event of an imminent terrorist threat and during and in the immediate aftermath of a terrorist attack within the

Figure 3.1 (*CONTINUED*) Executive order establishing the Department of Homeland Security.

(Continued)

3.2 Homeland Security Law, Regulations, and Executive Orders

United States and shall be the principal point of contact for and to the President with respect to coordination of such efforts. The Assistant to the President for Homeland Security shall coordinate with the Assistant to the President for National Security Affairs, as appropriate.

- (h) Continuity of Government. The Assistant to the President for Homeland Security, in coordination with the Assistant to the President for National Security Affairs, shall review plans and preparations for ensuring the continuity of the Federal Government in the event of a terrorist attack that threatens the safety and security of the United States Government or its leadership.
- (i) Public Affairs. The Office, subject to the direction of the White House Office of Communications, shall coordinate the strategy of the executive branch for communicating with the public in the event of a terrorist threat or attack within the United States. The Office also shall coordinate the development of programs for educating the public about the nature of terrorist threats and appropriate precautions and responses.
- (j) Cooperation with State and Local Governments and Private Entities. The Office shall encourage and invite the participation of State and local governments and private entities, as appropriate, in carrying out the Office's functions.
- (k) Review of Legal Authorities and Development of Legislative Proposals. The Office shall coordinate a periodic review and assessment of the legal authorities available to executive departments and agencies to permit them to perform the functions described in this order. When the Office determines that such legal authorities are inadequate, the Office shall develop, in consultation with executive departments and agencies, proposals for presidential action and legislative proposals for submission to the Office of Management and Budget to enhance the ability of executive departments and agencies to perform those functions. The Office shall work with State and local governments in assessing the adequacy of their legal authorities to permit them to detect, prepare for, prevent, protect against, and recover from terrorist threats and attacks.
- (l) Budget Review. The Assistant to the President for Homeland Security, in consultation with the Director of the Office of Management and Budget (the "Director") and the heads of executive departments and agencies, shall identify programs that contribute to the Administration's strategy for homeland security and, in the development of the President's annual budget submission, shall review and provide advice to the heads of departments and agencies for such programs. The Assistant to the President for Homeland Security shall provide advice to the Director on the level and use of funding in departments and agencies for homeland security-related activities and, prior to the Director's forwarding of the proposed annual budget submission to the President for transmittal to the Congress, shall certify to the Director the funding levels that the Assistant to the President for Homeland Security believes are necessary and appropriate for the homeland security-related activities of the executive branch.

GEORGE W. BUSH
THE WHITE HOUSE,
October 8, 2001.

Figure 3.1 (*CONTINUED*) Executive order establishing the Department of Homeland Security.

the United States of America, including the National Emergencies Act (50 U.S.C. 1601 et seq.) and section 301 of title 3, United States Code, and in furtherance of the proclamation of September 14, 2001, Declaration of National Emergency by Reason of Certain Terrorist Attacks, which declared a national emergency by reason of the terrorist attacks on the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States, I hereby order as follows:

Section 1. To provide additional authority to the Department of Defense and the Department of Transportation to respond to the continuing and immediate threat of further attacks on the United States, the authority under title 10, United States Code, to order any unit, and any member of the Ready Reserve not assigned to a unit organized to serve as a unit, in the Ready Reserve to active duty for not more than 24 consecutive months, is invoked and made available, according to its terms, to the Secretary concerned, subject in the case of the Secretaries of the Army, Navy, and Air Force, to the direction of the Secretary of Defense. The term "Secretary concerned" is defined in section 101(a)(9) of title 10, United States Code, to mean the Secretary of the Army with respect to the Army; the Secretary of the Navy with respect to the Navy, the Marine Corps, and the Coast Guard when it is operating as a service in the Navy; the Secretary of the Air Force with respect to the Air Force; and the Secretary of Transportation with respect to the Coast Guard when it is not operating as a service in the Navy.

EXECUTIVE ORDER: ON CRITICAL INFRASTRUCTURE PROTECTION

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, in the information age, it is hereby ordered as follows:

Section 1. Policy.

- (a) The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. The protection program authorized by this order shall consist of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. Protection of these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors.
- (b) It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations.

Sec. 2. Scope. To achieve this policy, there shall be a senior executive branch board to coordinate and have cognizance of Federal efforts and programs that relate to protection of information systems and involve:

- (a) cooperation with and protection of private sector critical infrastructure, State and local governments, critical infrastructure, and supporting programs in corporate and academic organizations;
- (b) protection of Federal departments, and agencies, critical infrastructure; and
- (c) related national security programs.

Sec. 3. Establishment. I hereby establish the "President's Critical Infrastructure Protection Board" (the "Board").

Figure 3.2 Executive order on critical infrastructure protection.

Sec. 2. To allow for the orderly administration of personnel within the armed forces, the following authorities vested in the President are hereby invoked to the full extent provided by the terms thereof: section 527 of title 10, United States Code, to suspend the operation of sections 523, 525, and 526 of that title, regarding officer and warrant officer strength and distribution; and sections 123, 123a, and 12006 of title 10, United States Code, to suspend certain laws relating to promotion, involuntary retirement, and separation of commissioned officers; end strength limitations; and Reserve component officer strength limitations.

On first glance, the Order takes the natural stance that our military complex is and always has been an integral part of the Homeland mission. Even so, the might and power of our military branches, coupled with the many governmental agencies dedicated to justice, homeland defense, emergency operations, and the like, make a homeland defense response more likely to be successful in the event of natural emergency. In 2017, the Order was amended, at Section 2, to permit appropriate military authority to order even retired military to active duty if the needs warrant the action.

3.2.4 Executive Order 13493 of January 22, 2009

Soon after his inauguration as president, Barack Obama reiterated his long-held view that the Guantanamo facility and its interrogation practices should be ended. In early 2009, he issued an order setting up a commission to end the status quo and seek transfer and other disposition of those residing in the facility. This promise was quite controversial. The order posed in part:

EXECUTIVE ORDER: IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Sec. 3. Policy Coordination. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive-1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 4. Cybersecurity Information Sharing.

- (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.
- (b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.
- (c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.
- (d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.
- (e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. Privacy and Civil Liberties Protections.

- (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

Figure 3.3 2013 Presidential proclamation.

(Continued)

- (b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.
 - (c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).
 - (d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.
- Sec. 6. Consultative Process. The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.
- Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure.
- (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.
 - (b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.
 - (c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.
 - (d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.
 - (e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the "preliminary Framework"). Within 1 year of the date of this order, and after coordination with

Figure 3.3 (CONTINUED) 2013 Presidential proclamation.

(Continued)

3.2 Homeland Security Law, Regulations, and Executive Orders

the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the "final Framework").

- (f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program.

- (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").
- (b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.
- (c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.
- (d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.
- (e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

Sec. 9. Identification of Critical Infrastructure at Greatest Risk.

- (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.
- (b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.
- (c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

Sec. 10. Adoption of Framework.

- (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states

Figure 3.3 (*CONTINUED*) 2013 Presidential proclamation.

(Continued)

whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

- (b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.
- (c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.
- (d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.
- (e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. Definitions.

- (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).
- (b) "Critical Infrastructure Partnership Advisory Council" means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.
- (c) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.
- (d) "Independent regulatory agency" has the meaning given the term in 44 U.S.C. 3502(5).
- (e) "Sector Coordinating Council" means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.
- (f) "Sector-Specific Agency" has the meaning given the term in Presidential Policy Directive-21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

Sec. 12. General Provisions.

- (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.
- (b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.
- (c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.
- (d) This order shall be implemented consistent with U.S. international obligations.
- (e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

Figure 3.3 (*CONTINUED*) 2013 Presidential proclamation.

REVIEW OF DETENTION POLICY OPTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, in order to develop policies for the detention, trial, transfer, release, or other disposition of individuals captured or apprehended in connection with armed conflicts and counterterrorism

3.2 Homeland Security Law, Regulations, and Executive Orders

operations that are consistent with the national security and foreign policy interests of the United States and the interests of justice, I hereby order as follows:

Section 1. Special Interagency Task Force on Detainee Disposition.

(a) Establishment of Special Interagency Task Force. There shall be established a Special Task Force on Detainee Disposition (Special Task Force) to identify lawful options for the disposition of individuals captured or apprehended in connection with armed conflicts and counterterrorism operations.⁴

The sum and substance of this decree were to find ways to end Guantanamo operations. However, while the president promised this policy during his first presidential campaign and in the early days of his administration, the decree has not been realized. By 2011, his position on Guantanamo was reversed. In January of that year, he signed the Defense Authorization Bill, essentially restricting the transfer of Guantanamo prisoners to other countries and the U.S. mainland. President Obama further clarified his position on Guantanamo in March 2011, when he signed Executive Order 13567.

3.2.5 Executive Order 13567 of March 7, 2011

Disposing of some of the world's most suspect figures in the underbelly of terrorism can be quite a challenge. President Obama, after over 2 years in office, essentially reverses his position on the closure of Guantanamo Bay by an order calling for periodic review and assessment of the prison's inhabitants. The more pertinent part of the order declares:

SECTION 1. SCOPE AND PURPOSE.

The periodic review described in Section 3 of this order applies only to those detainees held at Guantanamo on the date of this order, whom the interagency review established by Executive Order 13492 has (i) designated for continued law of war detention; or (ii) referred for prosecution, except for those detainees against whom charges are pending or a judgment of conviction has been entered.

This order is intended solely to establish, as a discretionary matter, a process to review on a periodic basis the executive branch's continued, discretionary exercise of existing detention authority in individual cases. It does not create any additional or separate source of detention authority, and it does not affect the scope of detention authority under existing law. Detainees at Guantanamo have the constitutional privilege of the writ of habeas corpus, and nothing in this order is intended to affect the jurisdiction of Federal courts to determine the legality of their detention.

In the event detainees covered by this order are transferred from Guantanamo to another U.S. detention facility where they remain in law of war detention, this order shall continue to apply to them.

Section 2. Standard for Continued Detention. Continued law of war detention is warranted for a detainee subject to the periodic review in Section 3 of this order if it is necessary.

At Section 2 of the order, the President makes plain that continued detention is within the discretionary authority of the United States under the law of war principles. President Obama has been severely critiqued for essentially maintaining the policy of former President George Bush. "The American Civil Liberties Union has been less than kind about the determination holding the decree shameful."⁵

Under the administration of Donald J. Trump, however, efforts to close Guantanamo had largely ended with a September 2018 proclamation revoking all previous efforts to close the facility. The Order states in part:

Sec. 2. Status of Detention Facilities at U.S. Naval Station Guantánamo Bay. (a) Section 3 of Executive Order 13492 of January 22, 2009 (Review and Disposition of Individuals Detained at the Guantánamo Bay Naval Base and Closure of Detention Facilities), ordering the closure of detention facilities at U.S. Naval Station Guantánamo Bay, is hereby revoked.

Homeland Security

(b) Detention operations at U.S. Naval Station Guantánamo Bay shall continue to be conducted consistent with all applicable United States and international law, including the Detainee Treatment Act of 2005.

(c) In addition, the United States may transport additional detainees to U.S. Naval Station Guantánamo Bay when lawful and necessary to protect the Nation.⁶

3.2.6 Executive Order 13846 of August 6, 2018

One of the prominent features in the homeland defense policy under the Trump Administration was the targeting of rogue nations and states that are supporters and promoters of terrorist activities throughout the world. No country has more egregiously offended in this manner than Iran. As a worldwide funder and promoter of terrorism, the efforts to deter this nation from these activities have only been partially successful. Aside from its usual saber-rattling, Iran has marched forward with a forbidden nuclear program which has been condemned by the United Nations. For other countries, like England and the United States, the efforts to minimize Iran's influence always include the use and application of sanctions. While President Obama was loosening these efforts and providing hundreds of millions of dollars to give incentives to end these terrorist activities, the Trump Administration re-imposed a multitiered sanction system. The Order reads in part:

I, DONALD J. TRUMP, President of the United States of America, in light of my decision on May 8, 2018, to cease the participation of the United States in the Joint Comprehensive Plan of Action of July 14, 2015 (JCPOA), and to re-impose all sanctions lifted or waived in connection with the JCPOA as expeditiously as possible and in no case later than 180 days from May 8, 2018, as outlined in the National Security Presidential Memorandum-11 of May 8, 2018 (Ceasing United States Participation in the Joint Comprehensive Plan of Action and Taking Additional Action to Counter Iran's Malign Influence and Deny Iran All Paths to a Nuclear Weapon), and to advance the goal of applying financial pressure on the Iranian regime in pursuit of a comprehensive and lasting solution to the full range of the threats posed by Iran, including Iran's proliferation and development of missiles and other asymmetric and conventional weapons capabilities, its network and campaign of regional aggression, its support for terrorist groups, and the malign activities of the Islamic Revolutionary Guard Corps and its surrogates...⁷

3.2.7 Homeland Security Act of 2002

At the congressional level, there was nothing but cooperation during the early stages of homeland security policy. By November 2002, Congress had passed the Homeland Security Act of 2002. The act was a comprehensive response to terror threats at every level. A summary of the act's provisions is outlined in its table of contents (Figure 3.4).

The Act lays out a national blueprint for homeland security and delineates the areas of vital national interest: borders; information and infrastructure; chemical, biological, and nuclear threats; and emergency preparedness and response. The Act has been subject to various revisions over the last 20 years regarding critical infrastructure and financial reporting and accountability problems, as well as various privacy clarifications. The Act is a work in progress by any measure. The Act has been subject to a host of legal and administrative critiques on various fronts, especially regarding abuse of privacy rights, overreach and improper application against U.S. citizens, outside any terrorist contexts and providing a structural court system, namely the FISA courts. The FISA courts have too often become rubber stamps for federal law enforcement and without sufficient external oversight, the parties to the Court who advocate claims have engaged in sweeping abuses.⁸

3.2 Homeland Security Law, Regulations, and Executive Orders

TITLE I — DEPARTMENT OF HOMELAND SECURITY		
	Sec. 101.	Executive department; mission.
	Sec. 102.	Secretary; functions.
	Sec. 103.	Other officers.
TITLE II — INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION		
	Sec. 201.	Under Secretary for Information Analysis and Infrastructure Protection.
	Sec. 202.	Functions transferred.
	Sec. 203.	Access to information.
	Sec. 204.	Information voluntarily provided.
TITLE III — CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR COUNTERMEASURES		
	Sec. 301.	Under Secretary for Chemical, Biological, Radiological, and Nuclear Countermeasures.
	Sec. 302.	Functions transferred.
	Sec. 303.	Conduct of certain public health-related activities.
	Sec. 304.	Military activities.
TITLE IV — BORDER AND TRANSPORTATION SECURITY		
	Sec. 401.	Under Secretary for Border and Transportation Security.
	Sec. 402.	Functions transferred.
	Sec. 403.	Visa issuance.
TITLE V — EMERGENCY PREPAREDNESS AND RESPONSE		
	Sec. 501.	Under Secretary for Emergency Preparedness and Response.
	Sec. 502.	Functions transferred.
	Sec. 503.	Nuclear incident response.
	Sec. 504.	Definition.
	Sec. 505.	Conduct of certain public health-related activities.
TITLE VI — MANAGEMENT		
	Sec. 601.	Under Secretary for Management.
	Sec. 602.	Chief Financial Officer.
	Sec. 603.	Chief Information Officer.
TITLE VII — COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; GENERAL PROVISIONS		
Subtitle A — Coordination with Non-Federal Entities		
	Sec. 701.	Responsibilities.
Subtitle B — Inspector General		
	Sec. 710.	Authority of the Secretary.
Subtitle C — United States Secret Service		
	Sec. 720.	Functions transferred.
Subtitle D — General Provisions		
	Sec. 730.	Establishment of human resources management system.
	Sec. 731.	Advisory committees.
	Sec. 732.	Acquisitions; property.
	Sec. 733.	Reorganization; transfer.
	Sec. 734.	Miscellaneous provisions.
	Sec. 735.	Authorization of appropriations.
TITLE VIII — TRANSITION		
	Sec. 801.	Definitions.
	Sec. 802.	Transfer of agencies.

Figure 3.4 Table of contents of the *Homeland Security Act of 2002*.

(Continued)

Homeland Security

	Sec. 803.	Transitional authorities.
	Sec. 804.	Savings provisions.
	Sec. 805.	Terminations.
	Sec. 806.	Incidental transfers.
TITLE IX — CONFORMING AND TECHNICAL AMENDMENTS		
	Sec. 901.	Inspector General Act.
	Sec. 902.	Executive Schedule.
	Sec. 903.	United States Secret Service.
	Sec. 904.	Coast Guard.
	Sec. 905.	Strategic National Stockpile and smallpox vaccine development.
	Sec. 906.	Select agent registration.
	Sec. 907.	National Bio-Weapons Defense Analysis Center.

Figure 3.4 (*CONTINUED*) Table of contents of the *Homeland Security Act of 2002*.

3.2.7.1 Homeland Security Act and Posse Comitatus

An often-overlooked section of the Homeland Security Act refers to the *Posse Comitatus Act* of 1878. The Posse Comitatus Act, passed June 18, 1878, essentially outlines limits on the federal government’s use of military force for the purposes of law enforcement. Section 886 of the Homeland Security Act refers to Posse Comitatus:

SEC 886(b) SENSE OF CONGRESS.—Congress reaffirms the continued importance of section 1385 of title 18, United States Code, and it is the sense of Congress that nothing in this Act should be construed to alter the applicability of such section to any use of the Armed Forces as a posse comitatus to execute the laws.⁹

Section 1385 of title 18 is the reference to Posse Comitatus and, per November 11, 2002, remarks of then-President George W. Bush, essentially the Homeland Security Act and Section 886(b) “does not purport to alter, modify, or otherwise affect the Posse Comitatus Act or judicial interpretations of that Act, and the executive branch shall construe this provision accordingly.”¹⁰

This becomes relevant and creates an interesting debate, however, as on October 1, 2002, just past the 1-year anniversary of 9/11, United States Northern Command (USNORTHCOM, or simply, NORTHCOM) was created.¹¹ A Unified Combatant Command (UCC) of the U.S. military, meaning it has multiple branches of the military under a single command, its purpose is to provide command and control of Department of Defense (DoD) homeland defense efforts and to coordinate defense support of civil authorities. In recent years, there has been a growing debate among politicians and government policymakers and scholars over what role, if any, the U.S. military should take in domestic operations. Though not exempt when deployed under federal service, the National Guard is exempt during peacetime or when specifically called on by state governors during crisis and disaster situations. The U.S. Coast Guard (USCG) is likewise exempt from Posse Comitatus.

Since its creation, NORTHCOM has aided in counter-drug operations as well as in response to Hurricane Katrina and multiple California and Colorado wildfires, as well as other similar regional domestic natural disaster events. Most recently, NORTHCOM provided logistical support during Hurricane Sandy when mid-Atlantic states like New York and New Jersey were devastated by severe coastal erosion and water and wind damage¹² (see Figure 3.5).

It remains to be seen what the ultimate policy on and role of NORTHCOM will be in responding to natural disasters or mass civil disturbances in the future.

3.2 Homeland Security Law, Regulations, and Executive Orders



Figure 3.5 Hurricane Sandy—Rockaway, New York. (Courtesy of FEMA.)

3.2.8 USA Patriot Act: USA Freedom Act of 2015

One of the most controversial pieces of legislation that arose from the turbulent post-9/11 period was the Patriot Act.¹³ The Patriot Act was developed out of the belief that our intelligence had been very poor prior to the attacks. It sought to remediate the perceived failures in intelligence and ensure such an attack would never occur again. Patriot Act proposals, swiftly drafted, were just as quickly signed and executed by President Bush on October 26, 2001. Given the intensity of the times, it is not surprising that a bill of this import found formal approval in so short a time span. The times influenced the aggressive nature of the bill. A thumbnail sketch of the act displays this inclination to expand or alter historic restrictions:

- *Information sharing*—The act liberalizes the sharing of intelligence information and removes most historical barriers to said sharing. Critics argue that the data will be used by other agencies for unrelated purposes or improper reasons.
- *Roving wiretaps*—The act permits the jurisdictional grant of one wiretap order that works or roves in multiple jurisdictions. Given the transiency of terrorists and the difficulties of dealing with diverse jurisdictions, the policy makes sense. Critics claim it will lead to an open-ended form of electronic surveillance.
- *Foreign intelligence and wiretaps*—The act liberalizes the grant and extent of this activity. New standards for use have been enacted. Critics claim this will lead to abuse, and given recent events since the election of Donald J. Trump, their concerns are well-founded.
- *Sneak and peek warrants*—In criminal parlance, “exigent” circumstances have always permitted law enforcement to search a house without a warrant. The act permits quick searches, without notification, of a suspected terrorist place of abode under an “any crime” provision. Critics note that the historic standard of these types of searches relates to loss of evidence or other exigency.
- *Material support*—The act expands the definition of support to include advice and counsel. Historically, “material” support related to economic or planning support that was central to the plot and plan. The idea of how one can support has been expanded. Critics claim this violates free speech.



Figure 3.6 President George W. Bush is joined by House and Senate representatives as he signs H.R. 3199, USA Patriot Improvement and Reauthorization Act of 2005, Thursday, March 9, 2006, in the East Room of the White House. (White House photo by Eric Draper.)

The Patriot Act was reauthorized in 2006 despite significant controversy¹⁴ (see Figure 3.6).

One of the act's most formidable allies was DHS. DHS publicly advocated for the passage of the reauthorization since it had amassed concrete examples of how effective the act had been in the apprehension of terrorists and the prevention of terror. In December 2005, DHS exhorted Congress to finish up its business relative to the act by noting

The Department of Homeland Security (DHS) benefits significantly from the USA Patriot Act and urges the United States Congress to reauthorize this proven tool in the global war on terror. The Patriot Act breaks down barriers to information sharing, enabling law enforcement and intelligence personnel to share information that is needed to help connect the dots and disrupt potential terror and criminal activity before they can carry out their plots. The broad information sharing provisions better enables U.S. Customs and Border Protection to screen international visitors and determine whether an apprehended alien presents a threat to security or public safety.¹⁵

Internet Exercise: To see the more important changes in the reauthorization bill, go to <http://www.govtrack.us/congress/bill.xpd?bill=h109-3199&tab=summary>.

During 2010–2011, the Patriot Act was reauthorized, although the debate was spirited and highly contentious on both sides of the aisle. The dissent even crossed party lines as liberals construed the broad sweep of police powers as being too unchecked, while conservatives concerned about the constitutional implications reached similar conclusions.¹⁶ In particular, the “roving wiretaps” provision, whereby investigators seek court orders that allow changing phone-number follow-ups without court scrutiny, was a stumbling block. Concerns also emerged regarding the sweeping data collection powers and the warrantless scrutiny of metadata and other communication information that the act seemed to allow without legal oversight. The act reiterated its three-part requirement when seeking the court order:

- Establishing probable cause that the target of the surveillance is a foreign power or agent of a foreign power
- Establishing probable cause that the device is being used or about to be used by a foreign power or agent of a foreign power
- Establishing that the actions of the target may have the effect of blocking their identification¹⁷

3.2 Homeland Security Law, Regulations, and Executive Orders

The reauthorized act also retained the more liberal and flexible standard when seizing the business records of a suspected terrorist, and instead of the historic “specific and articulable facts” requirement, a court could issue an order based on a “relevancy standard.”¹⁸

By 2015, and with the media explosion caused by the Edward Snowden defection to Russia and his release of documents exposing the powers exerted by the National Security Agency (NSA), the Central Intelligence Agency (CIA), and law enforcement under this act, Congress revised and retitled the act the “Freedom Act of 2015.”¹⁹ The act’s primary aim was

To reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes.²⁰

Internet Exercise: Review the Edward Snowden interview and timeline at <http://www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871>.

The provisions of the act now restrict broad, sweeping review of various forms of data without prior judicial approval from either traditional or specialized courts set up for said review. But political scandals and machinations continue to plague the various Acts and its established infrastructure. Even despite the protectionist language, the machinery of the FISA courts and judges are not overseen or scrutinized like other judicial venues or officers but operate in a sort of clandestine underworld where public scrutiny and any counter defense are nearly impossible. Despite numerous efforts to more aggressively regulate and keep in check, the FISA courts and corresponding process have produced a bevy of critics. Both liberal and conservative groups and political sponsors have called for revisions to the FISA process.²¹

There is an increasing call for the end of FISA courts or a reform that could reshape how it operates.²² Most critics of the FISA process bemoan its secrecy, its loose and nebulous standards for warrant applications and approval, its political influence, its complete lack of judicial or legislative oversight, and its tendency to rubber stamp all government petitions and requests.

Congress is still debating and scrutinizing changes to not only the FISA process but the USA Freedom and Patriot Acts. Both supporters and antagonists to these measures realize that the current workings of the FISA Court can no longer be tolerated.

Internet Exercise: Find out about the checkered history of FISA and its courts at: https://www.justice.gov/archive/ll/subs/q_support.htm

The current membership of the FISA court is shown in Table 3.1.²³

Controversial figure former Attorney General William Barr (Figure 3.7) even went so far to state that FISA courts were used improperly re: Trump and his connections to Russia with regard to the 2016 election, though many disagreed with his characterization.

Internet Exercise: For the full text of the U.S. Freedom Act, visit <https://www.congress.gov/bill/114th-congress/house-bill/2048>.

3.2.9 Specialized Laws

Aside from the broader legislation and regulations covering the world of homeland security, there are myriad other laws and rules promulgated on behalf of or by administrative agencies and departments entrusted with functions in homeland protection.

3.2.9.1 REAL ID Program

Concerns over the legitimacy and integrity of driver’s licenses resulted in the promulgation of a new DHS program—REAL ID.²⁴ The program sets minimum standards for the issuance of driver’s licenses, including

- Information and security features that must be incorporated into each card
- Proof of identity and U.S. citizenship or legal status of an applicant

Table 3.1 Current Membership of the FISA Court			
Judge	Judicial District/Circuit	Date Designated	Term expires
James E. Boasberg (Presiding)	District of Columbia/D.C.	May 19, 2014 (Presiding: January 1, 2020)	May 18, 2021
Rudolph Contreras	District of Columbia/D.C.	May 19, 2016	May 18, 2023
Anne C. Conway	Middle District of Florida/eleventh	May 19, 2016	May 18, 2023
Louis Guirola, Jr.	Southern District of Mississippi/fifth	July 2, 2019	May 18, 2026
James P. Jones	Western District of Virginia/fourth	May 19, 2015	May 18, 2022
Robert B. Kugler	District of New Jersey/third	May 19, 2017	May 18, 2024
Thomas B. Russell	Western District of Kentucky/sixth	May 19, 2015	May 18, 2022
George Z. Singal	District of Maine/first	May 19, 2019	May 18, 2026
John J. Tharp, Jr.	Northern District of Illinois/seventh	May 19, 2018	May 18, 2025
Anthony J. Trenga	Eastern District of Virginia/fourth	May 28, 2020	May 18, 2026



Figure 3.7 Former Attorney General William Barr.

- Verification of the source documents provided by an applicant
- Security standards for the offices that issue licenses and identification cards

Eventually, there will be an integration of other identification (ID) triggers such as social security and birth certificates; however, at this stage, the driver’s license has yet to be systematically governed. Critics of the act claim that it devises a national identity card program, but this criticism seems somewhat inaccurate. The provisions of the act reaffirm the preeminence of state governments in the matter of issuance and oversight. State compliance as of 2015 is shown in Figure 3.8.

3.2 Homeland Security Law, Regulations, and Executive Orders

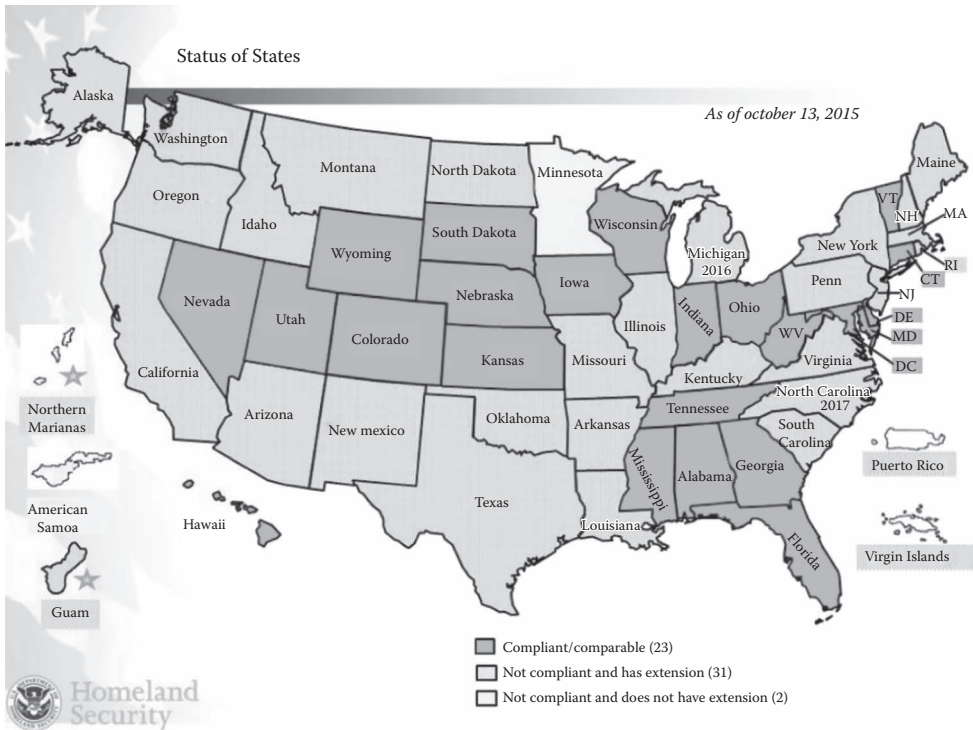


Figure 3.8 State compliance with REAL ID as of October 13, 2015.

Even DHS fosters an ambivalent and less than supportive view of the program due to costs and implementation challenges. In its Inspector General (IG) report, DHS remarked:

Potentially high costs pose a significant challenge to states in their efforts to implement REAL ID. Specifically, state officials considered REAL ID implementation costs prohibitive because of requirements such as the re-enrollment of all current driver's license and identification card holders and the new verification processes. Further, state officials in 17 of the 19 states we contacted indicated they needed more timely guidance from DHS to estimate the full cost of implementing REAL ID. State officials also said that REAL ID grants did not sufficiently mitigate the costs, and they viewed communication of grant information by DHS as ineffective.²⁵

With nearly a decade of legislative life, the REAL ID program has yet to fully materialize on a state-by-state level though it is getting closer. Implementation results have been dramatically mixed though there is a deadline of October 1, 2021. See Figure 3.9.



Figure 3.9 REAL ID deadline information campaign.

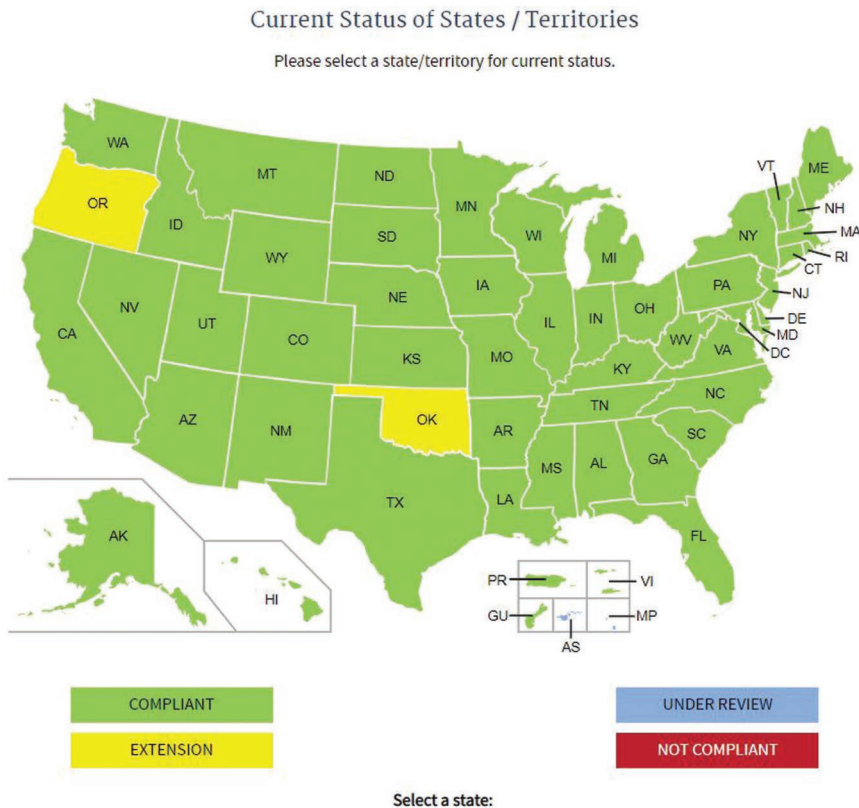


Figure 3.10 Current REAL ID status of U.S. states and territories.

By 2011, only 11 states had completely implemented the program.²⁶ As of 2020, the majority of the states are moving into compliance. See Figure 3.10.²⁷

Pace and commitment still differ among the states, but there is a noteworthy reduction in discussion as states are finding out that implementation, overall, is not as expensive as they thought and is achievable. States such as Maryland and Delaware, once committed, have completed the implementation of the 18 benchmarks needed to fulfill material compliance with the law within a year for only twice the grant monies provided by the federal government. Extrapolated out, that puts the total costs for implementing these key 18 REAL ID benchmarks in the range from \$350 million to \$750 million, an order of magnitude less than estimated previously. And with metrics in place, the story of REAL ID's value in securing against fraud is beginning to take shape not simply as theory but as reality.²⁸ The card design requirements are estimated at \$1.1 billion.²⁹ While compliance dates have been extended twice now, it appears unlikely that most states will ever be compliant with the diverse requirements of the act.³⁰

DHS continues to issue extensions to a great many states that have yet to comply and presently only designates American Samoa and Minnesota as fully noncompliant. Critics have also called into question the constitutionality of this sort of federalized oversight in the matter of national identity.³¹

3.2.9.2 Office of Biometric Identity Management (Formerly Office of US-VISIT)

The Office of Biometric Identity Management (OIBM), formerly known as U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT), resides in DHS and under the National

3.2 Homeland Security Law, Regulations, and Executive Orders

Protection and Programs Directorate and was established to track the entry and exit of travelers to the United States by biometric means—digital fingerprints and photographs. The guiding principles of OIBM are to

- Enhance the security of our citizens and visitors
- Facilitate legitimate travel and trade
- Ensure the integrity of the immigration system
- Protect the privacy of our visitors

The use of biometrics represents the cutting edge of identity assurance. By using unique physical characteristics, the agency can zero in on identity in a highly dependable way. OIBM uses biometric information to

- Check a person's biometrics against a watch list of known or suspected terrorists, criminals, and immigration violators
- Check against the entire database of all of the fingerprints DHS has collected since US-VISIT began to determine if a person is using an alias and attempting to use fraudulent identification
- Check a person's biometrics against those associated with the identification document presented to ensure that the document belongs to the person presenting it and not to someone else

Presently, the office is proposing a series of protocols for visitation. Upon a person's entry into the United States, a Customs and Border Protection officer (CBPO) uses inkless, digital finger scanners to scan both the left and right index finger of the person. The officer also takes a digital photograph.

OBIM's Biometric Support Center (BSC) provides DHS biometric verification services. Its primary mission is to provide expert fingerprint identification services to support DHS components along with federal, state, and local law enforcement agencies; intelligence agencies; and foreign partners.³²

To support this diverse customer base, OBIM employs contractor resources of highly skilled 10-print and latent fingerprint examiners operating 24 hours per day, 7 days per week to support critical immigration and border management missions, investigations, and identifications of potential persons of interest and unknown individuals. Specifically, the BSC supports OBIM's biometric verification capabilities by providing

- 10-print verification services to supplement IDENT's automated matching capabilities
- Latent print services involving the comparison and verification of known fingerprints with previously unidentified latent fingerprints
- Supplemental biometric services including IDENT biometric watchlist enrollments and biometric searches of IDENT for non-DHS stakeholders, including unknown deceased individuals, and biometric record maintenance³³

Internet Exercise: See the DHS instructional guidance for visitors at http://www.dhs.gov/xlibrary/assets/usvisit/US-VISIT_Updated_Entry_StepxStep.pdf.

3.2.9.3 Chemical Facilities

DHS has been actively involved in the oversight of chemical facilities due to their capacity to inflict widespread damage. Antiterrorism standards must be integrated in the design, plan, and operational security of designated chemical facilities. Congress, in passage of the 2007 Homeland Security reauthorization,³⁴ applies these standards because of the inherent risk to these facilities. DHS defines the risk as

Homeland Security

- The consequence of a successful attack on a facility (consequence)
- The likelihood that an attack on a facility will be successful (vulnerability)
- The intent and capability of an adversary in respect of attacking a facility (threat)

DHS establishes risk-based performance standards for the security of the country's chemical facilities. Covered chemical facilities are required to

- Prepare security vulnerability assessments, which identify facility security vulnerabilities
- Develop and implement site security plans, which include measures that satisfy the identified risk-based performance standards

Internet Exercise: Review the antiterrorism standards for chemical plants at <http://www.dhs.gov/cfats-risk-based-performance-standards>.

DHS publishes a list of chemical products of significant interest to the country and a list of assessment tools to ensure compliance.³⁵ Chemical facilities are construed as infrastructure.

3.2.9.4 Invention and Technology: The SAFETY Act

One of the best-kept secrets of the Homeland Security Act of 2002 was its desire to promote innovation in antiterrorism efforts. Innovation in technology is always a risky business. When the potential legal liabilities are added to the process of invention, such as being open to a lawsuit, the inventor is less aggressive. The *Support Antiterrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act)*³⁶ provides a safe harbor for the inventor and the product developer.

Internet Exercise: For a complete review of the SAFETY Act's many facets, see <https://www.safetyact.gov/pages/homepages/Home.do>.

It also provides a certification process whereby DHS approves a product for use in the fight against terrorism (see Figure 3.11).

As of 2015, hundreds of products and services have been approved. Some recent examples are shown in Figure 3.12.

To be an approved seller or certified developer of antiterrorism technology, the party must register. The process commences in a fairly simple way (see the registration document in Figure 3.13).

Internet Exercise: For numerous guides and instructions, visit the Safety Act website at <https://www.safetyact.gov> and access their "printer-friendly materials" list.

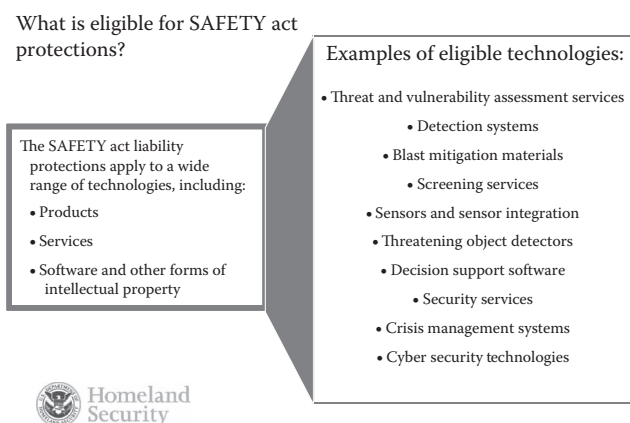


Figure 3.11 Technologies protected by the SAFETY Act.

3.3 Budgeting, Finance, and Funding in Homeland Security



Figure 3.12 Safety Act approved technologies listings. (https://www.safetyact.gov.)

3.3 Budgeting, Finance, and Funding in Homeland Security

Allocation of funds for operations depends on a multiplicity of factors. The age and history of a department influence funding; so too do the level of political importance and the social and cultural demand for a particular service or program. Priorities in budgeting are guided by many forces.³⁷ In the very short life of DHS, we have witnessed a radical evolution and an equally radical budgetary maturation. Over its 20-year lifespan, DHS has grown exponentially in matters of budget. In each of those years, while its numbers grew, it decided on a new and hopefully improved allocation formula. In addition, budget allotments vary year to year with emphases changing and challenges forcing or encouraging greater or less support depending upon need. What is certain, however, is that budgets correlate to demand and new concerns in the defense of the homeland. So, the earlier budgets of DHS are concerned less about cybersecurity problems than the more recent versions. From 2003 on, Congress and the executive branch looked closely at how best to allocate these precious funds. What has been patently obvious is that the investment in homeland security has not been cheap nor is it likely to get any less costly in the years ahead.

3.3.1 Budget Year: 2003

Since budgets are prepared a year in advance, the events of 9/11, happening close to the end of 2001, made any 2002 budget a factual impossibility. At best, the funds earmarked for homeland security in early 2002 would be strictly supplemental in design. Add to this the fact that DHS had yet to become a complete department with cabinet status, and the budget for the financial

The initial step in applying for the liability protections available under the SAFETY Act or for requesting a Pre-Application Consultation is to register with OSAI. Registration can be done electronically at the SAFETY Act website (<http://www.safetyact.gov>). You can also register by mail, using the forms included in this kit, or you can download an electronic copy of the form, complete it, and mail in the electronic document on a compact disc. Mailed registrations (hard copy or CD) should be sent to:

U.S. Department of Homeland Security
ATTN: Office of SAFETY Act
Implementation
245 Murray Lane, Building 410
Washington, DC 20528

Remember that physical mail sent to DHS is screened and processed, which may delay the Department's response to your submission. Registering with OSAI does not commit you to any further actions. The purpose of Registration is to establish an official point of contact for the Department to use in its interactions with you concerning your Technology and to create a unique identification number for you as a potential seller. This identifier will help the Department track and maintain your application. The SAFETY Act application process is designed to be flexible and to involve ongoing dialogue with the Applicant. Appropriate "points of contact" will facilitate this dialogue. The Applicant's point of contact may be any person you desire to coordinate your application and may include counsel, a representative of management, a technical expert or any other person you consider appropriate for this purpose.
(Registration Form on following page)

**REGISTRATION AS A SELLER
OF ANTITERRORISM TECHNOLOGY**

ACTION

R1. Purpose of Registration (*choose one*):
Initial Registration
Updated or Corrected Registration Information

REGISTRATION DATA

R2. Seller Name:
R3. Data Universal Numbering System (DUNS) Number (if available):

R4. North American Industry Classification System (NAICS) Code (if available):

POINT-OF-CONTACT INFORMATION

R5. Primary Point of Contact:
Name: _____
Address: _____
State/Province: _____ Country: _____ ZIP/Mail Code: _____
Telephone No.: _____ Fax No.: _____ E-mail: _____
E-mail Communication Authorized? Yes No

R6. Secondary Point of Contact (*optional*):
Name: _____
Address: _____
State/Province: _____ Country: _____ ZIP/Mail Code: _____
Telephone No.: _____ Fax No.: _____ E-mail: _____
E-mail Communication Authorized? Yes No

Figure 3.13 Registration as a seller of antiterrorism technology.

(Continued)

Instructions for Completing Registration Form:

ACTION

Item R1. Purpose of Registration

If your company or business unit has not previously registered with OSAI, check “Initial registration.” A company may file more than one registration; certain companies may wish to file multiple registrations if it has multiple business units selling dissimilar types of Technologies. As a rule, the entity that sells the Technology is the entity that should register.

If you are updating or correcting previous registration information, check “Updated or Corrected Registration Information.” OSAI strongly encourages you to keep your registration information up to date. In particular, be sure to notify OSAI of any changes in contact information.

REGISTRATION DATA

Item R2. Seller Name

Enter the legal name of your organization. If there will be business affiliates who will also be “sellers” of the Technology, please enter their legal names.

Item R3. Data Universal Numbering System (DUNS) Number

If your company has a nine-digit DUNS number, enter it here. If your company does not have a DUNS number, you do not need to provide one.

Item R4. North American Industry Classification System (NAICS) Code

NAICS Codes can be found in the official 2002 US NAICS Manual North American Industry Classification System—United States, 2002, available from the National Technical Information Service, (800) 553-6847 or (703) 605-6000, or directly from <http://www.census.gov/epcd/www/naics.html>.

POINT-OF-CONTACT INFORMATION

Item R5. Primary Point of Contact

Enter the name of the individual who will serve as the primary point of contact for interactions between your organization and OSAI. Provide a business address and telephone information for this person. OSAI prefers not to use personal or home contact information unless no other contact information is available. Include area codes and any non-U.S. country codes in telephone and fax numbers. If you wish to permit OSAI to correspond with this individual by e-mail, enter a valid e-mail address in the space provided.

The Applicant's point of contact may be any person you desire to coordinate your application and may include counsel, a representative of management, a technical expert or any other person you consider appropriate for this purpose.

Item R6. Secondary Point of Contact

Enter the name and contact information for an alternate point of contact in your organization.

OSAI will attempt to contact this person only if it is unable to reach the primary point of contact identified in item R5.

Figure 3.13 (*CONTINUED*) Registration as a seller of antiterrorism technology.

year (FY) 2002 was nothing more than a hodgepodge of supplemental additions to existing agencies. By March 2003, the initial allocations were targeted at

- Supporting first responders
- Defending against bioterrorism
- Securing America's borders
- Using twenty-first-century technology to secure the country (see Figure 3.14).

Homeland Security

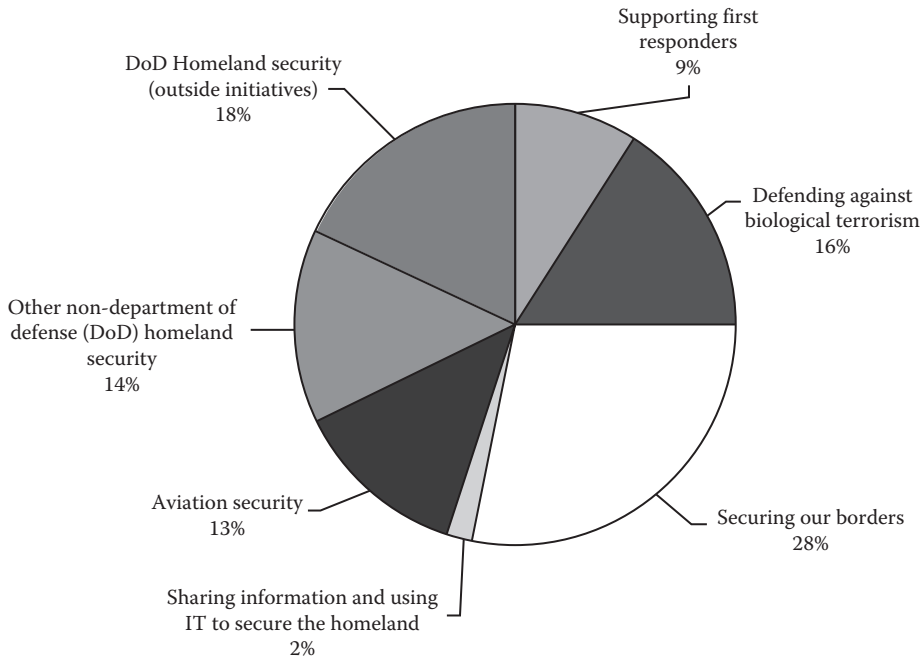


Figure 3.14 Homeland security distribution for FY 2003 by activity. (George W. Bush, *Securing Our Homeland: Strengthening our Future* [June 2003].)

The lack of a centralized cabinet-level agency was obvious as money was distributed during this budget cycle. Departments such as the Federal Emergency Management Agency (FEMA) and the departments of justice, health and human services, and energy all shared some portion of these homeland funds. In the 2003 budget cycle, the diversity of agencies participating foreshadowed the natural growing pains of an agency soon to be at the forefront (see Figure 3.15).

3.3.2 Budget Year: 2004

By mid-2003, the idea of a cabinet-level agency for homeland security had come to fruition. Like any new agency of government, special allotments—as start-up costs, so to speak—were issued. In addition, during the reorganization phase of 2003, a host of agencies and departments, such as the USCG and Secret Service, were merged into DHS. Hence, operational budgets had to reflect these costs of operation. By late 2003 and into 2004, a cabinet mentality was emerging in matters of homeland security. Yet, despite this developing culture, there were a series of adjustments, both structurally and fiscally, that DHS had to go through. The Office of Management and Budget charted this truncated approach by displaying how agencies and their functions often mix and merge together (see Figure 3.16).³⁸

Here, we witness how historic governmental entities, such as the Department of Defense (DoD), FEMA, the Federal Bureau of Investigation (FBI), and the USCG, would continue historic contributions to the protection of the homeland. In time, more and more of these bifurcated functions coalesced into DHS. By 2004, DHS had centered its attention on four areas of responsibility:

- *Border and transportation security*—encompasses airline security and inspection of cargo at points of entry into the United States to prevent unwanted individuals or weapons from entering the country.

3.3 Budgeting, Finance, and Funding in Homeland Security

Homeland security distribution of FY 2003 request by agency

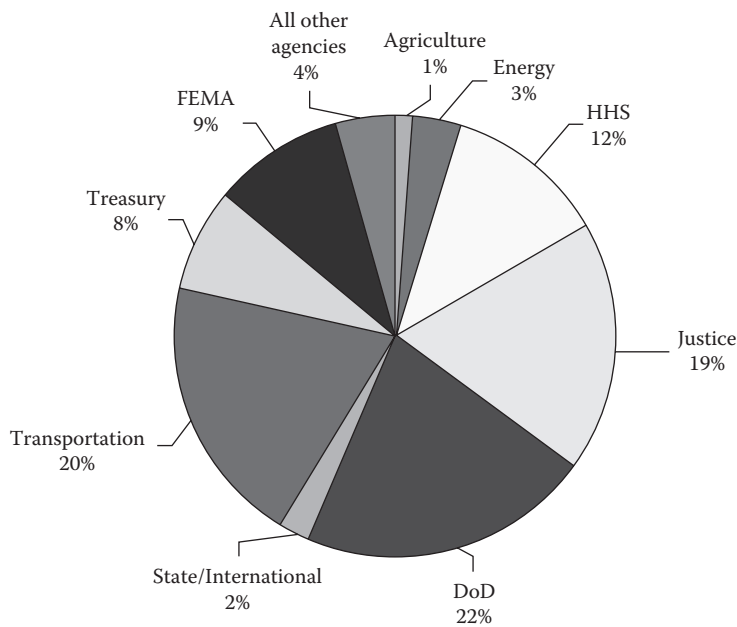


Figure 3.15 Homeland security budget distribution for FY 2003. (George W. Bush, *Securing Our Homeland: Strengthening our Future* [June 2003].)

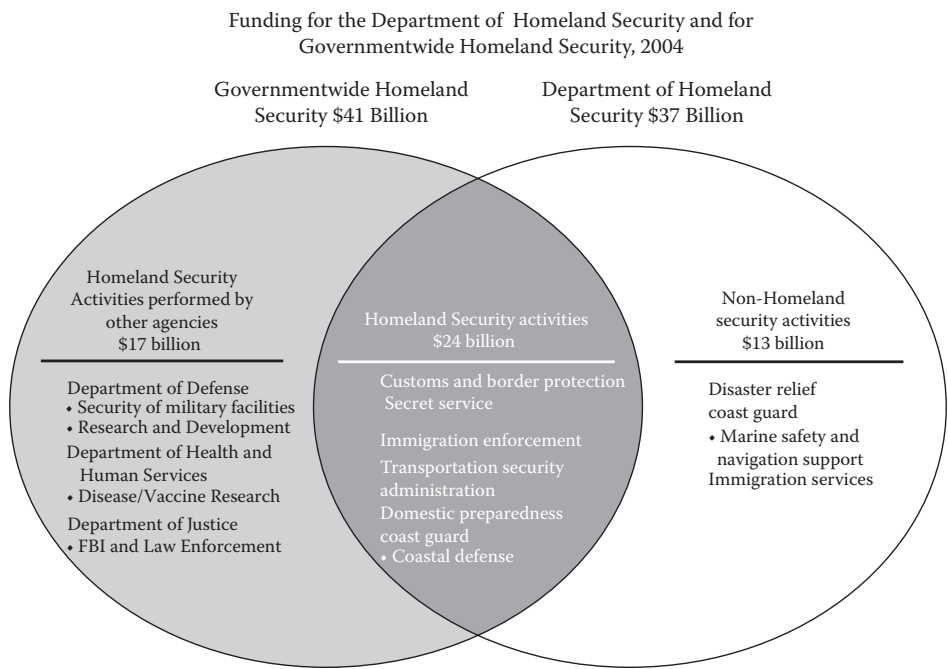


Figure 3.16 DHS funding and aligned governmental agency funding.

Homeland Security

- *Domestic counterterrorism*—consists largely of federal law enforcement and investigative activities that center on identifying and apprehending terrorists. Primary responsibility for these investigative activities rests with the Department of Justice’s FBI.
- *Protection of critical infrastructure and key assets*—includes ensuring the physical security of national landmarks and critical infrastructure (e.g., bridges and power plants) as well as the physical security of federal buildings and installations. The DoD receives the largest share of funding for this purpose.
- *Defense against catastrophic threats*—entails efforts to prevent terrorists from obtaining weapons of mass destruction (WMD: chemical, biological, or nuclear) and activities to mitigate the effects of such weapons if they are used. The Department of Health and Human Services (HHS) carries out most of those tasks.

With full department status, 2004 saw an extraordinary operational infusion. At the same time, the department stressed certain core values in its mission. Budgetary allotments mirrored these values, which were

- Securing the nation’s borders and transportation systems
- Securing the nation’s ports and ensuring safety in our waters
- Improving information analysis and infrastructure protection
- Advancing and harnessing science and technology
- Preparing for and responding to national emergencies
- Improving immigration services
- Other DHS activities and support

As for border and transportation, DHS doubled the budget from the previous year, which largely reflected the cache of new employees—approximately 60,000 individuals were hired. Many of these employees were sent directly to the nation’s airports to carry on the business of the Transportation Security Agency (TSA). Training funds were also widely disseminated to ensure a “same page” mentality among all agencies and departments, as well as state and local contributors responsible for homeland security.

As for ports and waterways, the emphasis was the same—to launch and support DHS initiatives. New maritime safety and security teams were developed; seed money for a maritime 911 was provided and multimillions were given to the USCG to shore up and increase its aging fleet (see Figure 3.17).

In the area of emergency response, the 2004 budget initiated the merger of FEMA and DHS, expanding and redefining the nature of disaster. From this budgetary cycle forward, DHS would see terror and hurricane from an identical prism. Billions were made available to develop a national stockpile for drugs, vaccines, and other medical supplies.



Figure 3.17 U.S. Coast Guard’s Deepwater logo.

DETAILED INFORMATION ABOUT THE STOCKPILE: HELPING STATE AND LOCAL JURISDICTIONS PREPARE FOR A NATIONAL EMERGENCY

An act of terrorism (or a large-scale natural disaster) targeting the U.S. civilian population will require rapid access to large quantities of pharmaceuticals and medical supplies. Such quantities may not be readily available unless special stockpiles are created. No one can anticipate exactly where a terrorist will strike, and few state or local governments have the resources to create sufficient stockpiles on their own. Therefore, a national stockpile has been created as a resource for all.

In 1999, Congress charged the HHS and the Centers for Disease Control and Prevention (CDC) with the establishment of the National Pharmaceutical Stockpile (NPS). The mission was to provide a resupply of large quantities of essential medical material to states and communities during an emergency within 12 hours of the federal decision to deploy.

The Homeland Security Act of 2002 tasked DHS with defining the goals and performance requirements of the Strategic National Stockpile (SNS) program as well as managing the actual deployment of assets. Effective on March 1, 2003, the NPS became the SNS program managed jointly by DHS and HHS. With the signing of the BioShield legislation, the SNS program was returned to HHS for oversight and guidance. The SNS program works with governmental and nongovernmental partners to upgrade the nation's public health capacity to respond to a national emergency. Critical to the success of this initiative is ensuring capacity is developed at federal, state, and local levels to receive, stage, and dispense SNS assets (see Figure 3.18).

The SNS is a national repository of antibiotics, chemical antidotes, antitoxins, life-support medications, IV administration, airway maintenance supplies, and medical/surgical items. The SNS is designed to supplement and resupply state and local public health agencies in the event of a national emergency anywhere and at any time within the United States or its territories.

The SNS is organized for flexible response. The first line of support lies within the immediate response 12-hour Push Packages. These are caches of pharmaceuticals, antidotes, and medical supplies designed to provide rapid delivery of a broad spectrum of assets for an ill-defined threat in the early hours of an event. These Push Packages are positioned in strategically located, secure warehouses, ready for immediate deployment to a designated site within 12 hours of the federal decision to deploy SNS assets.

If the incident requires additional pharmaceuticals and/or medical supplies, follow-on vendor managed inventory (VMI) supplies will be shipped to arrive within 24–36 hours. If the agent is well defined, VMI can be tailored to provide pharmaceuticals, supplies, and/or products specific to the suspected or confirmed agent(s). In this case, the VMI could act as the first option for an immediate response from the SNS program.



Figure 3.18 A national repository of life-saving pharmaceuticals and medical material.



Figure 3.19 National Biodefense Analysis and Countermeasures Center.

To advance the use of science and technology in the fight against terrorism, the 2004 budget proposed a sevenfold increase over the previous year. The key emphasis was on the detection of radiological, chemical, nuclear, and biological threats. A total of \$137 million was earmarked for detection systems at points of entry and within the transportation infrastructure, and \$365 million was allotted for the detection and prevention of biological attacks and the implementation of a new department exclusively dedicated to these tasks—the National Biodefense Analysis and Countermeasures Center (NBACC) (see Figure 3.19).

Internet Exercise: Read a recent report on the progress, successes, and struggles in the development of the NBACC at <http://www.fas.org/sgp/crs/homsec/RL32891.pdf>.

ABOUT NATIONAL BIODEFENSE ANALYSIS AND COUNTERMEASURES CENTER

NATIONAL BIODEFENSE ANALYSIS AND COUNTERMEASURES CENTER

The gross space, or entire footprint of the facility, is expected to be about 160,000 square feet. This includes administrative areas, BSL-2, 3, and 4 laboratory spaces, air-handling equipment space, security controls, and other supporting features. NBACC expects to employ 120 researchers and support staff.

NBACC INTERIM CAPABILITY

An interim capability for the NBFAC has been established in partnership with the FBI and the U.S. Army at the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID). The BTCC supports risk assessment and threat characterization research in other established government and nongovernmental laboratories, including USAMRIID. The permanent NBACC facility will be located at Fort Detrick, Maryland, once construction is completed in 2008.

SAFETY MEASURES

The NBFAC will employ state-of-the-art biosafety procedures and equipment to prevent biological material from escaping into the environment. Rigorous safeguards protect those who work in the laboratory and the surrounding community.

Once construction is complete, the NBACC facility will feature proven safeguards, applying time-tested rigorous design standards, special safety equipment, and exacting operating procedures to govern all research.

3.3 Budgeting, Finance, and Funding in Homeland Security

These standards, equipment, and procedures have been demonstrated to provide the highest level of safety in existing laboratories elsewhere at Fort Detrick and throughout the United States.

The security of the NBACC facility will always be safeguarded through strict control access for those working in the laboratory facility. To gain access to select agents, individuals must complete an in-depth background investigation and demonstrate competency in safety and security equipment and procedures in accordance with both Department of Homeland Security regulations and federal law.

By locating the NBACC facility at Fort Detrick, the Department leverages the security provided by the U.S. Army military garrison with biocontainment-specific capabilities to create a controlled, secure environment.

See Figure 3.20³⁹

In the area of information sharing and analysis and infrastructure protection, the DHS budget of 2004 funded shared databases, provided essential mechanisms for shared intelligence, and erected a 24/7 intelligence and warning system. The 2004 budget delivered funds to states and localities to develop partnerships and information-sharing systems as well as finances to establish compatible communication systems. The budget provided the necessary funds to create the Homeland Security Advisory Warning System (see Figure 3.21).

Finally, the 2004 budget recognized the dramatic need for improved immigration services. In particular, the budget fully recognized the negative impacts caused by chronic and continuous backlogs.

By 2011, however, the National Advisory System, the color-coded version, had been scrapped in favor of the National Terrorism Advisory System (NTAS) (see Figure 3.22).

This new system provides timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector about terrorist threats. See Figure 3.23⁴⁰ for a sample alert format.

Finally, the 2004 budget recognized the dramatic need for improved immigration services. In particular, the budget fully recognized the negative impacts caused by chronic and continuous backlogs.

Internet Exercise: For the documentary side of the immigration application, see <http://www.uscis.gov/forms>.

3.3.3 Budget Year: 2005

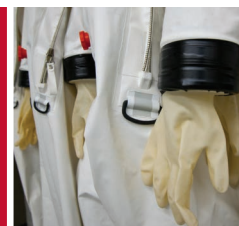
Expenditures for homeland defense reflected the growth and priorities of the agency. Now in its second full year of operation, DHS, aside from support for the agency and its structure, targeted specific activities and honed its purpose. What is undeniably certain is that growth in the budget continued unabated⁴¹ (see Figure 3.24).

As each year passes, the department searches for best practices and discerns where the threat is most imminent. By 2005, DHS stressed ports and maritime security, streamlined preparedness models, and enhanced biodefense practices through the increased use of science and technology, as well as providing enough funding for the training of first responders at the state and local levels.

Maritime concerns clearly took center stage in 2005 with the budget addressing numerous initiatives associated with port and shipping safety and security. Some examples worth noting are

- The Container Security Initiative (CSI), which focuses on prescreening cargo before it reaches our shores. The first phase of CSI focused on implementing the program at the top 20 foreign ports, which ship approximately two-thirds of the containers to

NATIONAL BIODEFENSE ANALYSIS AND COUNTERMEASURES CENTER (NBACC)



Location: National Interagency Biodefense Campus, Fort Detrick, MD

Core Competencies: Aerobiology; Safe, Secure and Compliant Biocontainment Operations; Bioforensics; Comparative Medicine; Quality Management; Genomics and Bioinformatics; and Broad Capabilities in Bacteriology, Virology, Toxinology

Accreditations/Registrations: ISO 17025 Quality (A2LA), CDC/USDA Select Agent for BSL-2, 3, and 4, AAALAC International, Institutional Biosafety Committee, Nuclear Regulatory Commission, Drug Enforcement Administration Controlled Substance, Alcohol and Tobacco Tax and Trade Bureau Industrial Alcohol User Permit

Key Customers: Law Enforcement, DHS and Homeland Security Enterprise Biodefense Stakeholders

NBACC is the first national laboratory created by the Department of Homeland Security. NBACC provides a continuously available national security biocontainment laboratory capability to address newly identified biological threats. NBACC's mission is to provide the scientific basis for the characterization of biological threats and bioforensic analysis to support attribution of their planned or actual use. NBACC components include the National Bioforensic Analysis Center (NBFAC) and the National Biological Threat Characterization Center (NBTC).

NBACC Operations and Support

- Provides safe and compliant operations for more than 50,000 square feet of Bio Safety Level (BSL) 2, 3, and 4 laboratories, including continuous operational support to law enforcement.
- Maintains Centers for Disease Control and Prevention (CDC) and the U.S. Department of Agriculture (USDA) Biological Select Agent and Toxin Program compliant biosafety laboratories, including CDC/USDA inspections.
- Conducts a "Work for Others" program that makes the NBACC national security biocontainment capabilities more broadly available to federal agencies.

- Maintains Defense Security Service compliance.

NBFAC Accomplishments

- From fiscal year (FY) 2011 to the first half of FY 2018, NBFAC supported 197 federal law enforcement investigations and analyzed more than 8,891 samples.
- NBFAC continues to provide 24/7, "Always Available" bioforensic analyses and support for traditional forensic analyses within biocontainment for federal law enforcement with "purpose built" bioforensic casework laboratories, dedicated and vetted technical staff, and ISO 17025 accredited processes and assays at BSL-1, 2, 3, and 4.
- NBFAC identifies and characterizes biological agents in evidentiary samples with simultaneous analyses using orthogonal agent based assays, which include bacterial and viral culture, polymerase chain reaction and immunoassays as well as methods-based capabilities that include genomics (whole genome sequencing and bioinformatics analysis), electron microscopy, and mass spectrometry (MS).
- In FY2018, ISO 17025 accredited human genotyping using next generation sequencing.
- NBFAC's agent and methods-based capabilities at BSL-1, 2, 3, and 4 provide flexibility in the identification and characterization of a wide range of biological agents that include traditional, non-traditional, emerging, genetically engineered, and synthetic biological agents.

NBTC Accomplishments

- NBTC has provided timely and high quality data on the characteristics of biological threat agents and dual use technologies to inform DHS and HSE policy and decision-making before and in response to new biological threats.
- From fiscal year (FY) 2011 to the first half of FY 2018, NBTC has provided scientific data to address 85 traditional agent knowledge gaps to inform and improve both the understanding of biological hazards faced by the country and preparedness planning to mitigate the impact of a biological event on the homeland.
- In response to the largest Ebola outbreak recorded, Ebola stability and disinfection data critical to understanding the potential risk of the virus transmission through contaminated surfaces was used to inform decontamination methods, waste disposal practices, and risk assessments for first responders.

Contact

Questions? Email questions@nbacc.dhs.gov for more information.

Office of National Laboratories (ONL)



Figure 3.20 ONL's information sheet on the NBACC.

the United States. Phase II expands the program to additional ports based on volume, location, and strategic concerns. Phase III further increases security at the highest-risk ports. The three core elements of CSI are to

- Identify high-risk containers. Automated targeting tools are used to identify containers that pose a potential risk for terrorism, based on advanced information and strategic intelligence.

3.3 Budgeting, Finance, and Funding in Homeland Security



Figure 3.21 Levels of the Homeland Security Advisory System.



Figure 3.22 The Homeland Security Advisory Warning System was replaced by the National Terrorism Advisory System (NTAS).

- Prescreen and evaluate containers before they are shipped. Containers are screened as early as possible in the supply chain, generally at the port of departure.
- Use technology to prescreen high-risk containers to ensure that screening can be done rapidly without slowing down the movement of trade. This technology includes large-scale x-ray and gamma-ray machines and radiation detection devices.
- The Customs-trade Partnership Against Terrorism (C-TPAT), which began in November 2001, is another essential cargo security effort. C-TPAT focuses on partnerships all along the entire supply chain, from the factory floor, to foreign vendors, to land borders and seaports.
- Customs and border protection targeting systems aid in identifying high-risk cargo and passengers. The budget included an increase of \$20.6 million for staffing and technology acquisition to support the National Targeting Center (NTC), trend analysis, and the automated targeting systems (ATS) (Figure 3.25).
- The US-VISIT program's first phase is being deployed at 115 airports and 14 seaports. US-VISIT expedites the arrival and departure of legitimate travelers, while making it more difficult for those intending to do us harm to enter our nation.



National Terrorism Advisory System
Alert
www.dhs.gov/alerts

DATE & TIME ISSUED: XXXX

SUMMARY

The Secretary of Homeland Security informs the public and relevant government and private sector partners about a potential or actual threat with this alert, indicating whether there is an “imminent” or “elevated” threat.

DURATION

An individual threat alert is issued for a specific time period and then automatically expires. It may be extended if new information becomes available or the threat evolves.

DETAILS

- This section provides more detail about the threat and what the public and sectors need to know.
- It may include specific information, if available, about the nature and credibility of the threat, including the critical infrastructure sector(s) or location(s) that may be affected.
- It includes as much information as can be released publicly about actions being taken or planned by authorities to ensure public safety, such as increased protective actions and what the public may expect to see.

AFFECTED AREAS

- This section includes visual depictions (such as maps or other graphics) showing the affected location(s), sector(s), or other illustrative detail about the threat itself.

HOW YOU CAN HELP

- This section provides information on ways the public can help authorities (e.g. camera phone pictures taken at the site of an explosion), and reinforces the importance of reporting suspicious activity.
- It may ask the public or certain sectors to be alert for a particular item, situation, person, activity or developing trend.

STAY PREPARED

- This section emphasizes the importance of the public planning and preparing for emergencies before they happen, including specific steps individuals, families and businesses can take to ready themselves and their communities.
- It provides additional preparedness information that may be relevant based on this threat.

STAY INFORMED

- This section notifies the public about where to get more information.
- It encourages citizens to stay informed about updates from local public safety and community leaders.
- It includes a link to the DHS NTAS website <http://www.dhs.gov/alerts> and <http://twitter.com/NTASAlerts>

If You See Something, Say Something™. Report suspicious activity to local law enforcement or call 911.

The National Terrorism Advisory System provides Americans with alert information on homeland security threats. It is distributed by the Department of Homeland Security. More information is available at: www.dhs.gov/alerts. To receive mobile updates: www.twitter.com/NTASAlerts

If You See Something Say Something™ used with permission of the NY Metropolitan Transportation Authority.

Figure 3.23 Sample DHS National Terrorism Advisory System alert.

- Radiation detection monitors screen passengers and cargo coming into the United States. The budget includes \$50 million for the next generation of screening devices (Figure 3.26).
- Aerial surveillance and sensor technology increases the effectiveness of the more than 12,000 Border Patrol agents deployed along the northern and southern borders, and it also supports other missions, such as drug interdiction (Figure 3.27).

3.3 Budgeting, Finance, and Funding in Homeland Security

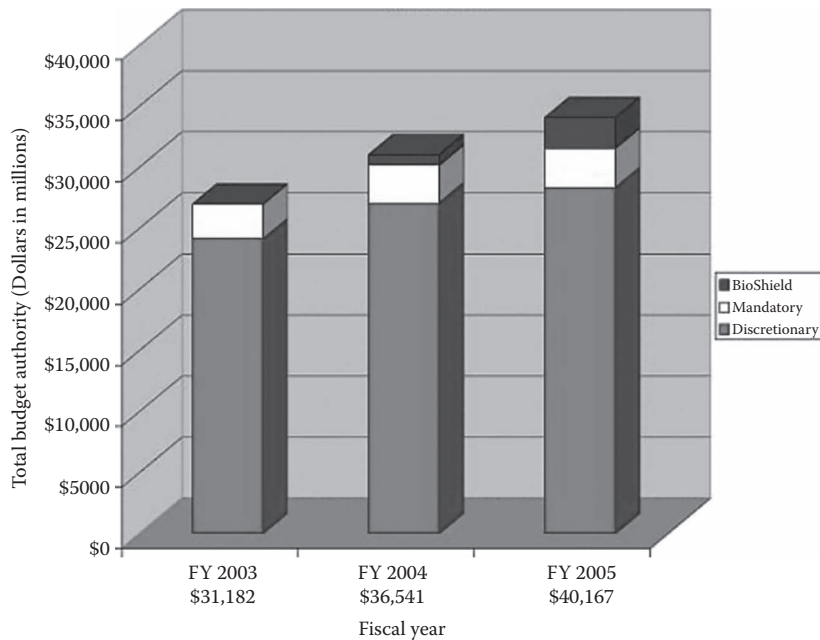


Figure 3.24 DHS funding 2003–2005.



Figure 3.25 President George W. Bush tours the National Targeting Center (NTC) in Reston, Virginia, February 6, 2004. The NTC is part of Homeland Security’s Bureau of Customs and Border Protection, and the center provides analytical research support for counterterrorism efforts.

On the biodefense front, DHS advanced a mix of technology with proven practices in the fight against terrorism. Project BioShield purchased and collected essential vaccines and medications for use in the event of a biological attack. Particular emphasis was given to vaccines for small-pox and anthrax exposure. In addition, just as in the nuclear theater, DHS expended millions developing and installing monitoring equipment that detects biological threats (Figure 3.28).

In the area of preparedness, the 2005 budget developed and implemented the National Incident Management System (NIMS) program and corresponding systems (Figure 3.29).

Homeland Security

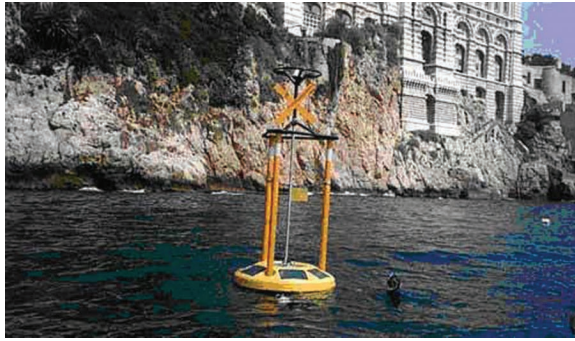


Figure 3.26 A radiation monitor at the entrance of a port. (Courtesy of International Atomic Energy Agency.)



Figure 3.27 Cargo ship at sea.



Figure 3.28 Example of a monitoring system installed at a port where cargo containers are unloaded. (www.whitehouse.gov.)

3.3 Budgeting, Finance, and Funding in Homeland Security

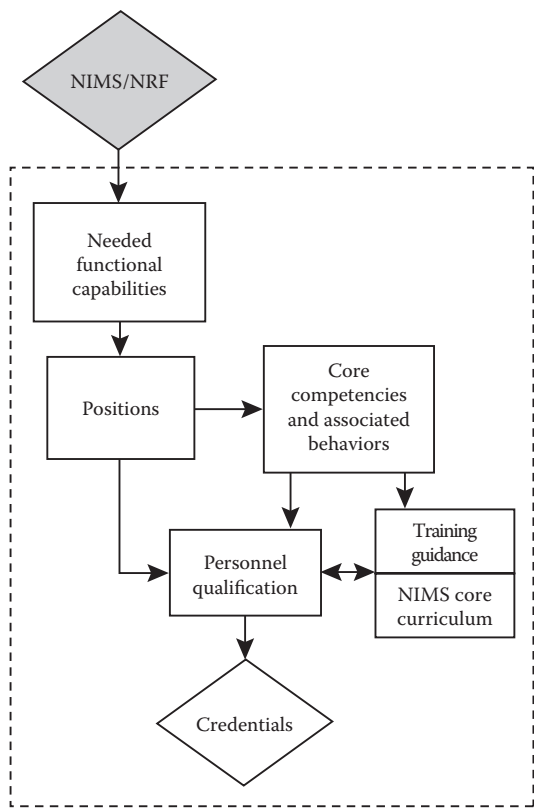


Figure 3.29 Department of Homeland Security, National Incident Management System (NIMS): 5-year NIMS training plan: National Integration Center (NIC), Incident Management Systems Integration (IMSI) Division, 4.

NIMS is a program for all critical infrastructures and provides agencies, hospitals, and justice facilities with a plan of action that protects the facility and prevents attacks. In most jurisdictions, legislation now requires that staff and managers be educated in NIMS practices. NIMS trains and certifies both the personnel and agency.

In the areas of information and infrastructure protection, the budget reflected increased concerns over cyberterrorism (Figure 3.30). Expending nearly \$68 million on the National Cyber Security Division—a center that identifies and analyzes cyber vulnerability—the 2005 budget appreciated the extraordinary implications of threats in the virtual world.

Cybersecurity threats generally fall into the following categories:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information (PII)-related incidents
- Unwanted disruption or denial of service
- Unauthorized use of a system for processing or storing data
- Changes to system hardware, firmware, or software characteristics without the owner’s knowledge, instruction, or consent

The budget also delivered funding to develop threat assessment tools for infrastructure protection. Strategic assessments of threats to the country’s critical infrastructures and key assets,



Figure 3.30 October is National Cyber Security Awareness Month.

including 168,000 public water systems, 300,000 oil and natural gas production facilities, 4,000 offshore platforms, 278,000 miles of natural gas pipelines, 361 seaports, 104 nuclear power plants, 80,000 dams, and tens of thousands of other potentially critical targets across 14 diverse critical infrastructure sectors, are a central aim of the budget.

The 2005 budget contributed more than just funding to the vision and plan of homeland security. Just as critically, the budget tied budgetary practices to general principles of accountability and assessment. In other words, the budget evaluated the efficacy of the disbursement considering present strategic directions, future ambition of the departments, and overall accountability. As such, the budget became performance driven. Referring to a loop, the 2005 budget seeks to tie disbursement to effectiveness, as charted in Figure 3.31.

The goals and mission of DHS are evaluated considering budgetary disbursement,⁴² an example of which is shown in Figure 3.32.

3.3.4 Budget Year: 2006

Expenditures for homeland security continue an upward trek in 2006. When compared with 2005, the amount allotted for homeland protection is up 7%⁴³ (see Figure 3.33).

As each year passes, DHS expends more and more of its energy measuring and evaluating the effectiveness of its programs. In addition, it assesses all of its practices in light of changing demands and new detectable threats. To illustrate, the budget established the Domestic Nuclear Detection Office (DNDO), which seeks to detect and report efforts to acquire and deploy nuclear materials. The strategic objectives of the DNDO are to

- Develop the global nuclear detection and reporting architecture
- Develop, acquire, and support the domestic nuclear detection and reporting system
- Fully characterize detector system performance before deployment
- Facilitate situational awareness through information sharing and analysis
- Establish operation protocols to ensure detection leads to effective response

3.3 Budgeting, Finance, and Funding in Homeland Security

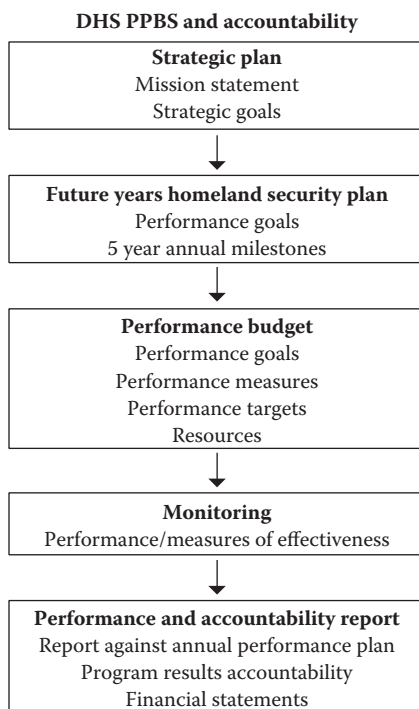


Figure 3.31 Department of Homeland Security: Performance budget overview FY 2005, page 3.

Performance Goal: Establish a fully capable Command, Control, Operations, and Information Exchange System.

Measure: Percentage increase in time efficiency of issuance of information and warning advisories.	Fiscal Year	FY 2003	FY 2004	FY 2005
	Target	None	Baseline	Increase by 10%
	Actual	None	t.b.d.	t.b.d.
Program: Homeland Security Operations Center	\$ Thousands	None	\$20,878	\$36,212
Lead Organization: Information Analysis and Infrastructure Protection Directorate	FTE	None	None	8

Performance Goal: Increase time efficiency of issuance of information and warnings advisories by fifty percent.

Measure: Time efficiency of issuance of information and warning advisories	Fiscal Year	FY 2003	FY 2004	FY 2005
	Target	None	Baseline	Increase by 10%
	Actual	None	t.b.d.	t.b.d.
Program: Information & Warning Advisories	\$ Thousands	None	\$79,314	\$93,056
Lead Organization: Information Analysis and Infrastructure Protection Directorate	FTE	None	None	202

Performance Goal: Reduction of "general" warnings as compared to "at risk" warnings by sixty percent from 2003 levels.

Measure: Reduction of general warnings, as compared to "at risk" warnings	Fiscal Year	FY 2003	FY 2004	FY 2005
	Target	None	Baseline	20%
	Actual	None	t.b.d.	t.b.d.
Program: Infrastructure Vulnerability & Risk Assessment	\$ Thousands	None	\$95,173	\$85,033
Lead Organization: Information Analysis and Infrastructure Protection Directorate	FTE	None	None	85

Figure 3.32 Performance goals for DHS.

- Conduct a transformational research and development program
- Provide centralized planning, integration, and advancement of U.S. government nuclear forensics programs

Homeland Security

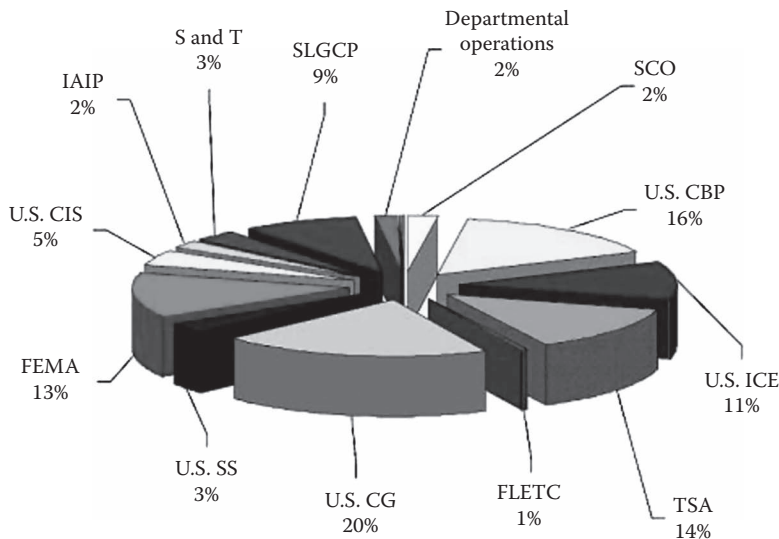


Figure 3.33 DHS budgetary lines—FY 2006.

The budget additionally consolidated a host of research, development, and testing offices into the Science and Technology Directorate. In the area of border security, the line items recognize the increasing importance of safety and security at the country's geographic borders. Substantial funding for WMD detection equipment became available, as well as the institution of America's Shield Initiative, which employs electronic surveillance equipment at our borders. Long-range radar technology, which detects and intercepts aircraft illegally entering the United States, also received support.

The 2006 budget is generous in the area of law enforcement by supporting a host of initiatives, including

- The Armed Helicopter for Homeland Security Project—a project to provide the USCG with more firepower
- Federal Air Marshal Service—\$689 million for increased safety in the air
- Response boats, cutters—increased budgeting for USCG upgrades (Figure 3.34)
- Flight deck and crew training in self-defense

The budget recognized the need for assistance to first responders by erecting the Office of State and Local Government Coordination and Preparedness (SLGCP). In the area of communications and first response, the Office of Interoperability and Compatibility will fund emergency systems to ensure compatible communication systems. As unbelievable as it may seem, emergency responders often cannot talk to some parts of their own agencies—let alone communicate with agencies in neighboring cities, counties, or states. DHS instituted the SAFECOM program, which plans and implements interoperability solutions for data and voice communications.

Internet Exercise: View the Introduction to SAFECOM Presentation accessible from SAFECOM's website at <http://www.dhs.gov/safecom/about-safecom>.

Interoperability will succeed when the following five elements are achieved:

- Gain leadership commitment from all disciplines (e.g., emergency medical services [EMS], fire rescue response, and law enforcement)

3.3 Budgeting, Finance, and Funding in Homeland Security



Figure 3.34 U.S. Coast Guard at work. (U.S. Navy photo by Kelly Newlin.)

- Foster collaboration across disciplines through leadership support
- Interface with policymakers to gain leadership commitment and resource support
- Use interoperability solutions regularly
- Plan and budget for ongoing updates to systems, procedures, and documentation

Communication upgrades are in store for the USCG. Rescue 21 will replace aging and often cumbersome equipment for coast guard service (see Figure 3.35).

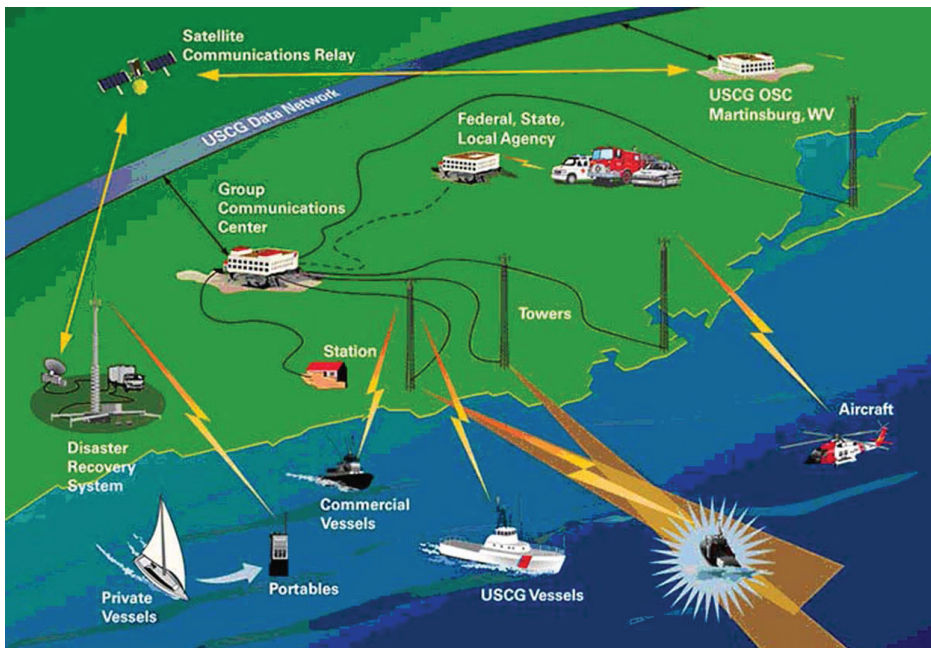


Figure 3.35 Rescue 21.



Figure 3.36 The Homeland Security Operations Center. (www.whitehouse.gov.)

How it works:

- A call for help is sent.
- Direction finding (DF) equipment from one or more high sites computes the direction from which the signal originated or the line of bearing (LOB).
- Distress audio and the LOB are sent to the closest ground center(s).
- Appropriate resources are dispatched to respond immediately—even across regional boundaries.⁴⁴

Other programs emphasized in the 2006 budget include internal funding for more efficient DHS operation, including human resources, information sharing, electronic data capability, high-speed operational connectivity, and sufficient funding to operate the Homeland Security Operations Center (HSOC) (Figure 3.36).

Internet Exercise: To evaluate the 2006 budget in light of performance, visit http://www.dhs.gov/xlibrary/assets/Budget_PBO_FY2006.pdf.

3.3.5 Budget Year: 2007

As DHS entered its fourth year of department status, it was clear that it continued to strive for efficiency in both an internal and an external sense. DHS understands being prepared has much to do with prevention and mitigation of disaster in any form. To anticipate terror or plan for natural disasters, the department is forced to target its resources and focus its efforts on what is yet to happen. In this sense, the department is becoming a proactive, rather than a strictly reactionary, entity.

In the world of preparedness, the 2007 budget expended a good deal of investment. Millions were directed to the National Preparedness Integration program, a historic FEMA responsibility involving catastrophic planning, emergency communication improvements, and command and control alignment. FEMA received \$29 million to reinforce its readiness, mitigation, response, recovery, and national security programs under the initiative Strengthen Operational Capability. Upgrades to the Emergency Alert System (EAS) were also provided. EAS is an integral part of the public alert and warning system in the United States. It provides the president and other authorized federal, state, and local officials with the capability to transmit an emergency message to the public during disasters or crises. The national EAS, regulated by the Federal Communications Commission (FCC), is administered by DHS through FEMA.

3.3 Budgeting, Finance, and Funding in Homeland Security

Internet Exercise: For a comprehensive critique of the EAS system, see <http://www.gao.gov/new.items/d07411.pdf>.

The Coast Guard received \$60 million to enhance its National Capital Region Air Defense program (Figure 3.37).⁴⁵

Border security and reform of the immigration process continued to see substantial support in the budgetary process up to and including 2007. Cutting-edge technology was employed across the borders using electronic surveillance. Coupled with technology and surveillance was an infusion of funds, some \$459 million, to hire and train 3,000 new border agents (Figure 3.38).



Figure 3.37 An HH65 Coast Guard helicopter passes by the Washington Monument during a National Capital Region Air Defense training mission. (U.S. Coast Guard news photo.)



Figure 3.38 U.S. Border Patrol on duty. Department of Homeland Security, Washington, D.C.

Homeland Security

Additional fencing, detention beds, and work location and employment verification programs were also included in the 2007 budget.

Maritime and cargo continued to be a forefront concern in the budgetary process in matters of homeland security in the year 2007. The use of technology continued to be heavily supported when it came to the detection of explosives, nuclear materials, and WMD (Figure 3.39).

At America's ports, the threat that may emerge from cargo is a story likely to be told in the future. Law enforcement cannot inspect all the cargo that enters our ports, since manual inspection would be ludicrous given the sheer volume of incoming goods. Advanced radiography is considered a sensible solution to inspecting the millions of cargo containers that reach the American shores every year. The 2007 budget funds Cargo Advanced Automated Radiography Systems⁴⁶ (see Figure 3.40).

Information sharing takes a preeminent position in the 2007 budget. In the world of IT infrastructure, DHS stressed the common and reliable e-mail systems, the centralization of data centers, the modernization of desktops and workstations, and the update of voice, video, and wireless infrastructure. Nearly \$50 million was geared to the Office of Intelligence and Analysis and the Operations Directorate, where threat information is analyzed and disseminated and other information pertinent to homeland threat is sent to all partners and governmental entities. Of particular interest in 2007 was the Secure Border Initiative. The goals of the initiative are

- More agents to patrol our borders, secure our ports of entry, and enforce immigration laws
- Expanded detention and removal capabilities to eliminate “catch and release” once and for all



Figure 3.39 Explosive detection system. Department of Homeland Security, Washington, D.C.

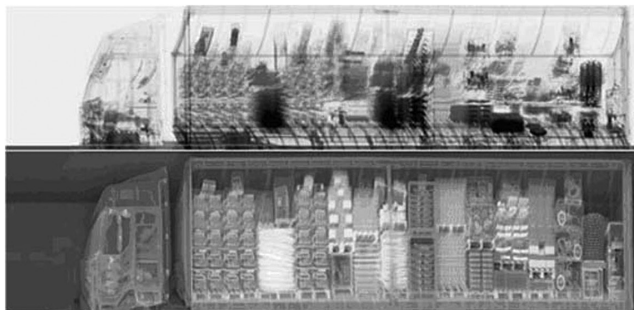


Figure 3.40 Radiographic image of a truck.

3.3 Budgeting, Finance, and Funding in Homeland Security

- A comprehensive and systemic upgrading of the technology used in controlling the border, including increased manned aerial assets, expanded use of unmanned aerial vehicles (UAVs), and next-generation detection technology
- Increased investment in infrastructure improvements at the border—providing additional physical security to sharply reduce illegal border crossings
- Greatly increased interior enforcement of our immigration laws—including more robust worksite enforcement

The initiative’s focus on fencing is quite a challenge; from autos and trucks to pedestrians, the erection of a border fence across the continental United States is a project in the making⁴⁷ (Figure 3.41).

Finally, DHS will continue to infuse funds into its own internal operations in order that it might be an agency for the twenty-first century. Special disbursements for human services and procurements were made.

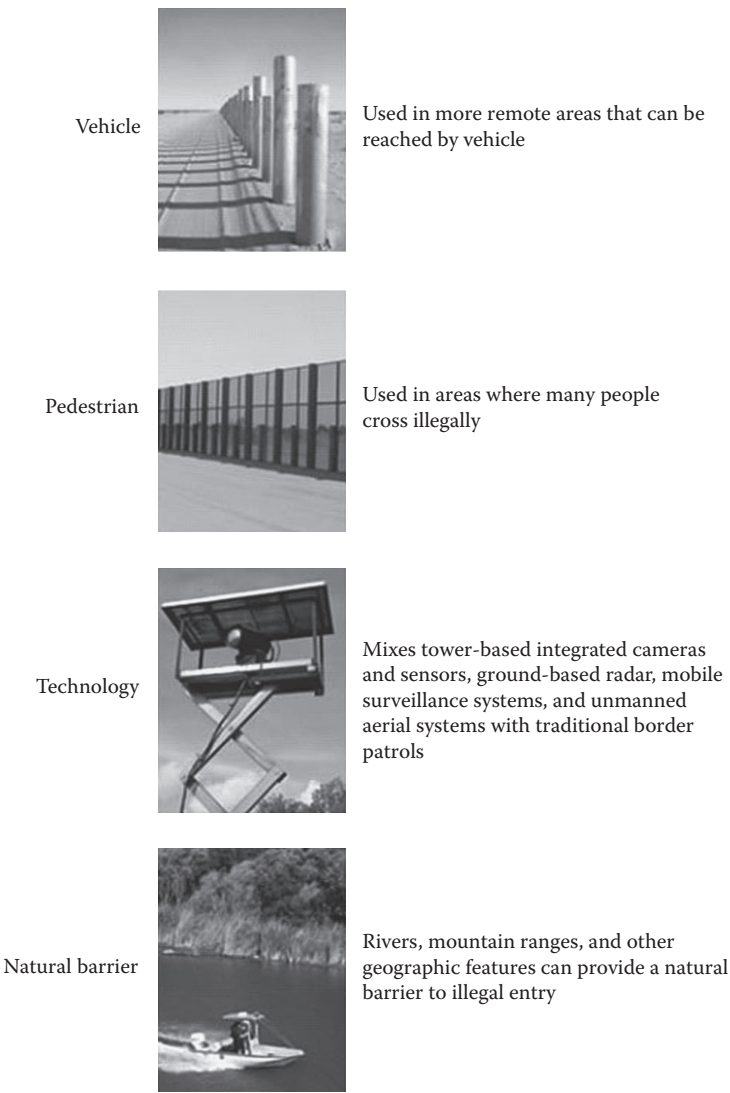


Figure 3.41 DHS barrier and border techniques. (www.dhs.gov.)

3.3.6 Budget Year: 2008

In its fifth year of operation, DHS had had sufficient time to examine its practices, to weigh and assess the effectiveness of its plan and operation, and to act and react to existing and novel challenges. What is plain is that budgets continue to rise, and threats manifest an uncanny capacity to evolve. DHS needs to stay sharp and always on the offense to fend off a very dangerous world. Congress and the president seem to appreciate the financing demand that DHS naturally entails. Since its inception, the budget has matured⁴⁸ (see Figure 3.42).

The mission of DHS stays firm and resolute in this budgetary process—first and foremost, to protect the country from danger and threat. Another 3,000 Border Patrol agents were added during this cycle. The Transportation Security Administration saw increased funding for explosives detection, document processes, and the new identification programs.

Border protection received strong support in the 2008 budget. SBInet, a program instituted under the Secure Border Initiative, was slated to provide form and structure to the 6,000 miles of border in need of protection. The goal of this program, by technology, infrastructure, staffing, and response resource, was the integration of border protection into a single comprehensive border security suite for the department. U.S. CBP was to serve as executive agent for the department's SBInet program (Figure 3.43). The program was canceled in January 2011.⁴⁹

Foreign visitors will be subject, depending on the location of entry, to biometric screening or other advanced fingerprint imprint analysis (Figure 3.44).

Included in the budget were funds to launch the Secure Flight system. Secure Flight will match limited passenger information against government watch lists to identify known and suspected terrorists, prevent known and suspected terrorists from boarding an aircraft, facilitate legitimate passenger air travel, and protect individual privacy. Secure Flight will

- Identify known and suspected terrorists
- Prevent individuals on the No-Fly List from boarding an aircraft
- Identify individuals for enhanced screening
- Facilitate passenger air travel by providing a fair, equitable, and consistent matching process across all aircraft operators

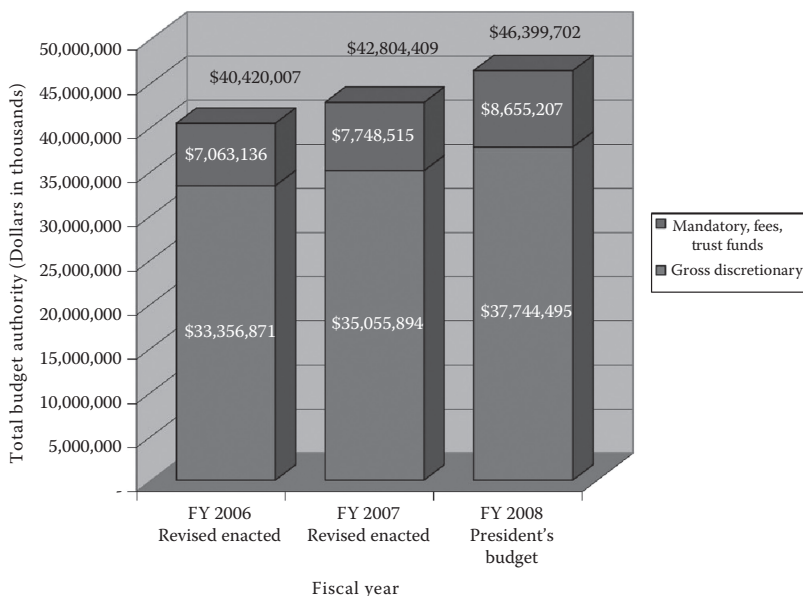


Figure 3.42 Budget growth: 2006–2008.

3.3 Budgeting, Finance, and Funding in Homeland Security



Figure 3.43 U.S.–Mexico Border. Mexico is on the right. (www.cpg.gov.)



Figure 3.44 A biometric fingerprint device. (Courtesy of FBI.)

In addition to Secure Flight's efforts to improve the efficiency and effectiveness of passenger pre-screening, TSA, in conjunction with Secure Flight, has developed the Joint Analysis Center. This center is co-located within the SOC and uses encounter match data to perform broader aviation security analysis. Analysts located at Secure Flight work jointly with TTAC (Transportation Threat Assessment and Credentialing) and TSA OI (Office of Intelligence) analysts to use passenger vetting results from Secure Flight and other programs to identify trends and patterns in aviation security.⁵⁰

At our commercial ports and points of entry, the 2008 budget demonstrated innovation at the technological level. Advanced spectroscopic portal systems will scan and screen 98% of incoming containers at the end of the budget cycle. Raytheon delivered the first prototype and portal for commercial use in 2006 (see Figure 3.45).

The Secure Freight program (Figure 3.46) received its start-up costs of \$15 million in the 2008 budget. Secure Freight screens foreign containers bound for U.S. ports for radiological and nuclear risk. Containers are screened before leaving a foreign port. DHS and the Department of Energy will partner with international terminal operators, ocean carriers, and host governments.



Advanced Spectroscopic Portal (ASP)



The Advanced Spectroscopic Portal (ASP) is an advanced nuclear screening portal system designed to identify and interdict the illegal entry of nuclear devices and materials into the United States.

Benefits

Critical defense tool for the Department of Homeland Security (DHS) and the Domestic Nuclear Detection Office (DNDO)

Senses nuclear materials at various points of entry into the United States, as well as other locations such as domestic checkpoints and rail lines

Capable of screening cars, trucks, cargo containers and mail

Modular architecture allows system to be mounted in several configurations

Multiple detector types ensure high gamma and neutron sensitivity over full range of usage conditions

Designed to minimize false alarms that would unnecessarily impede the flow of border traffic and commerce

System incorporates advanced threat identification algorithms

Designed to Counter Nuclear Threat

Covert nuclear attack is the foremost threat facing the United States today. The safety of the nation depends upon its ability to design and field systems to detect and interdict smuggled nuclear weapons and materials. For this reason, the ASP is a high-priority program within DHS and a key component of DNDO and other federal national nuclear detection initiatives to meet homeland security needs. By enhancing the country's early detection capabilities, ASP detectors address the threat of radiological dispersal devices, improvised nuclear devices or a nuclear weapon being used by terrorists inside the United States.

Upgrade Over Current Detector Portals

Since Sept. 11, 2001, the Bureau of Customs and Border Protection has deployed nearly 600 first-generation Radiation Portal Monitors at manned ports of entry, international mail and express consignment courier facilities, land border crossings, airports and seaports. As a point of reference, DHS reports that 360,000 vehicles, 5,100 trucks and containers, 2,600 aircraft, and 600 vessels cross into the United States at more than 600 points of entry every day.

Built with available technology, these first-generation Radiation Portal Monitors are unable to distinguish between legitimate naturally occurring radioactive materials such as

fertilizer and bananas that are not harmful, and illicit materials that pose a threat. These situations necessitate secondary screening, which is manpower intensive and slows the flow of commerce. Therefore, a more discriminating primary screening system — the ASP — is needed.

Figure 3.45 Raytheon's advanced spectroscopic portal.

Containers arriving at participating seaports overseas will be scanned with both nonintrusive radiographic imaging and passive radiation detection equipment placed at terminal arrival gates. Sensor and image data gathered regarding containers inbound to the United States will be encrypted and transmitted near real time to the NTC operated by DHS's Customs and Border Protection.

As for infrastructure, the 2008 budget heartily supported a continuation of the Domestic Nuclear Detection Office and established an Office of Innovation in the Directorate of Science and Technology (S&T). The S&T Directorate is the intellectual arm of DHS and a place of innovation and invention. Partnering with the private sector, national laboratories, universities,



Figure 3.46 Secure freight initiative in Hamburg, Germany.

and other government agencies, the office promotes the use of high technology in support of homeland security.

The budget allotted a significant increase for chemical site security programs.

Internet Exercise: Find out about the registration process for chemical facilities at <http://www.dhs.gov/chemical-security-laws-and-regulations>.

From the vantage point of emergency preparedness, DHS works hard to finalize the acculturation of FEMA. FEMA has been an agency under siege since the days of Katrina, and it has taken heartfelt introspection and diligence to reset the agency moorings. The consolidation of FEMA into DHS caused further consternation for personnel. As a result, FEMA revisited its vision and overall mission and, on completion, was given an additional \$100 million to carry out these adjusted aims. FEMA will zero in on these activities:

- Incident management
- Hazard mitigation
- Operational planning
- Disaster logistics
- Service to disaster victims
- Public disaster communication
- Continuity programs

More than \$3.2 billion was made available for state and local preparedness training. A total of \$3.2 billion was allotted for state and local preparedness expenditures as well as assistance to firefighters. The Homeland Security Grants, Infrastructure Protection, Assistance to Firefighters, and Public Safety Interoperable Communications (PSIC) grant programs fund activities necessary to support the National Preparedness Goal and related national doctrine, such as the NIMS, National Response Plan (NRP), and the National Infrastructure Protection Plan (NIPP). Funds requested through these programs will (1) provide critical assistance to state and local homeland security efforts, (2) support resources available through other federal assistance programs that center on first-responder terrorism preparedness activities, and (3) deliver support to all state and local first-responder organizations (Figure 3.47).

Finally, the 2008 budget financed internal operations with the hope of improved efficiency at DHS. Funds were directed to internal oversight of personnel, further consolidation of duplicate



Figure 3.47 CBRN response drill.

functions and offices, a permanent Office of Chief Procurement, and increased funding for oversight and audit provided by the Office of the Inspector General (OIG).

3.3.7 Budget Years: 2009–2010

Not surprisingly, increased allocations for DHS activities continue their upward march. While it is not difficult to anticipate increasing expenditures for homeland security, it is not as simple to predict where portions of money will go for innovation or changed focus. To be sure, DHS will always have an operational side. Then too, DHS will most likely continue the bulk of its initiatives. Government can change, but the likelihood of radical change or whole-scale change is very remote. For 2009 and 2010, DHS stayed true to its basic mission. Some of the proposed highlights were

- Aggressive increase in Border Patrol—2,200 new agents and further funding for Secure Flight (Figure 3.48)
- TSA funds for ID programs and crew vetting as well as a new program that tracks international students
- An automated, electronic system of worker verification, E-Verify (see Figure 3.49)
- \$10 million in increased funding for the Federal Law Enforcement Training Center (FLETC) relating to border enforcement
- Increased funding for the U.S. Secret Service for equipment that detects WMD and other attacks
- Improvised explosive device (IED) research

3.3.8 Budget Years: 2011–2012

Two forces were at work in the budgets posed by DHS officials and adopted or under legislative consideration. First, for the first time in its administrative life, there is actually a discussion

3.3 Budgeting, Finance, and Funding in Homeland Security

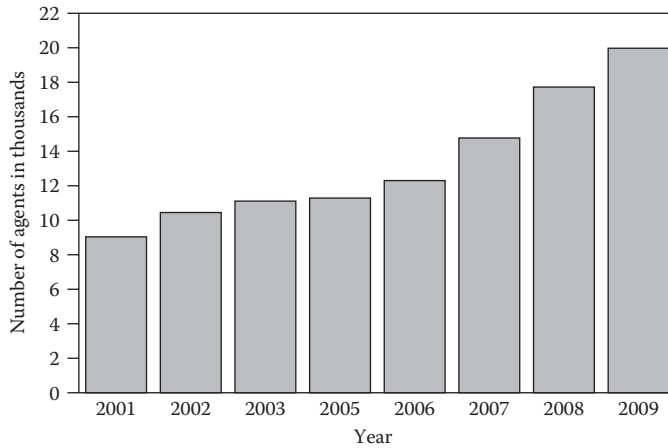


Figure 3.48 Border patrol staffing, 2001–2009. (www.white.gov/omb/budget/fy2009/homeland.html.)



Figure 3.49 E-verify logo.

of better efficiencies and trimmed funding for DHS.⁵¹ Across the governmental horizon, there is bleeding in federal overspending, and each agency is being asked to cull where it can. For example, DHS is required to conduct due diligence on its payments to vendors to ensure proper amounts and reduce duplication in payments.⁵² DHS is required to make public and publish incorrect payments. A few examples of high-dollar overpayments are charted in Figure 3.50.⁵³

DHS continues its high-level emphasis on technology as a tool of efficiency. At the same time, despite the technological advances, the agency continues to splurge on employees and increased staff across various departments. What is clear is that budgets are moving across a relative flat-line—at least in a governmental sense. From 2010 to 2011, the department's funds dipped \$118,000,000, though the proposed 2012 budget seeks an increase of those losses. See Figure 3.51⁵⁴ for a 3-year comparison.

Over the same 3-year period, one can glean some targeted spending as well as some deemphasis. The proposed 2012 budget reduces funding to the following categories:

- Citizenship and Immigration Services
- FEMA grant programs
- FLETC
- Domestic Nuclear Detection Office

While the reductions are not fantastic, these cuts reflect support for ICE activities in the present administration as well as the law enforcement sector in its training activities. FEMA is likely just tapped out given the disaster calendar.

All other remaining functions and offices retain their upward trend in budgetary allocation (see Figure 3.52).⁵⁵

Homeland Security

Department of Homeland Security
Current Status of Outstanding High-Dollar Overpayments Reported on the Previous Secretary's High-Dollar Overpayments Report
for the Quarter Ending December 31, 2011

Debts Sent to the Treasury Offset Program for Collection											
A	B	C	D	E	F	G	H	I	J	K	L
Component	Recipient Type	City and State	Program(s) Responsible	Recovery Actions Taken or Planned	Payment Date	High's Overpayment Date Identified	Amount Paid	Correct Amount	Recovered Amount	Outstanding Balance	Days Outstanding as of December 31, 2011
FEMA	INDIVIDUAL	Seabrook, TX	Individuals and Households Payments	Recoupment package sent to individual. Debt later sent to the Treasury Offset Program for collection.	November 11, 2008	September 30, 2010	\$19,239.54	\$0.00	\$0.00	\$19,239.54	457
USCG	ENTITY	Miami, FL	Air Station Miami	Contacted vendor who confirmed overpayment. Vendor added to USCG "Do Not Pay List" with automatic offset of overpayment on next invoice. Debt sent to Treasury Offset Program for collection.	September 25, 2010	January 10, 2011	\$76,740.37	\$38,177.37	\$0.00	\$38,563.00	355

Totals	\$95,979.91	\$38,177.37	\$0.00	\$57,802.54
--------	-------------	-------------	--------	-------------

Debts Under Collection by DHS											
A	B	C	D	E	F	G	H	I	J	K	L
Component	Recipient Type	City and State	Program(s) Responsible	Recovery Actions Taken or Planned	Payment Date	High's Overpayment Date Identified	Amount Paid	Correct Amount	Recovered Amount	Outstanding Balance	Days Outstanding as of December 31, 2011
FEMA	ENTITY	Carson City, NV	Homeland Security Grant Program	Additional supporting documentation received from grantee. FEMA reviewing for sufficiency with resolution expected by January 2012. DHS senior management to elevate this issue to FEMA senior management to ensure timely resolution. State is appealing improper payment.	September 30, 2009	August 5, 2010	\$27,609.10	\$0.00	\$0.00	\$27,609.10	513
FEMA	ENTITY	District of Columbia, DC	Homeland Security Grant Program	Program office completed a review of recipient provided documentation and fully discussed results with grant recipient. Proper support was found for an additional \$1,348,108.50 of the original payment. A collection bill for the remaining \$643,115.65 was sent.	August 19, 2009	July 28, 2010	\$3,133,009.25	\$2,489,893.60	\$0.00	\$643,115.65	521
USCG	INDIVIDUAL	Seattle, WA	Coast Guard Pay & Personnel Center/Direct	Notice of Overpayment sent to member and copy to Servicing Personnel Office. Collection by payroll deductions began.	November 11, 2008	June 15, 2011	\$8,903.21	\$1,051.71	\$1,023.96	\$6,827.54	199

Totals	\$3,169,521.56	\$2,490,945.31	\$1,023.96	\$677,552.29
Grand Totals	\$3,265,501.47	\$2,529,122.68	\$1,023.96	\$735,354.83

Figure 3.50 High-dollar overpayments still in the collection process.

3.3 Budgeting, Finance, and Funding in Homeland Security

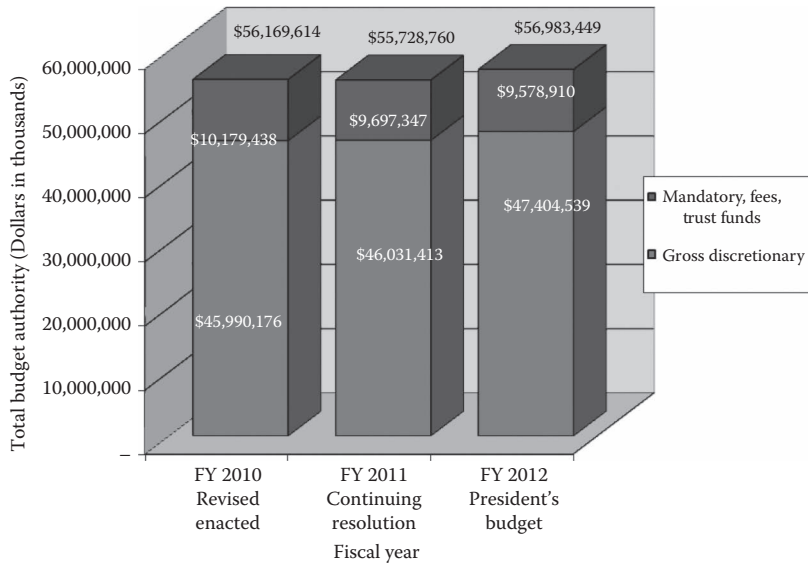


Figure 3.51 U.S. Department of Homeland Security, total budget authority.

TOTAL BUDGET AUTHORITY BY ORGANIZATION
Gross Discretionary, Mandatory, Fees, and Trust Funds

	FY 2010 Revised Enacted ¹	FY 2011 Continuing Resolution ²	FY 2012 President's Budget	FY 2012 +/- FY 2011	FY 2012 +/- FY 2011
	\$000	\$000	\$000	\$000	%
Departmental Operations³	\$ 809,531	\$ 800,931	\$ 947,231	\$ 146,300	18%
Analysis and Operations (A&O)	333,030	335,030	355,368	20,338	6%
Office of the Inspector General (OIG)	113,874	129,874	144,318	14,444	11%
U.S. Customs & Border Protection (CBP)	11,540,501	11,544,660	11,845,678	301,018	3%
U.S. Immigration & Customs Enforcement (ICE)	5,741,752	5,748,339	5,822,576	74,237	1%
Transportation Security Administration (TSA)	7,656,066	7,649,666	8,115,259	465,593	6%
U.S. Coast Guard (USCG)	10,789,076	10,151,543	10,338,545	187,002	2%
U.S. Secret Service (USSS)	1,710,344	1,722,644	1,943,531	220,887	13%
National Protection and Programs Directorate (NPPD)	2,429,455	2,432,756	2,555,449	122,693	5%
Office of Health Affairs (OHA)	136,850	139,250	160,949	21,699	16%
Federal Emergency Management Agency (FEMA)	6,200,618	6,181,718	6,218,433	36,715	1%
FEMA: Grant Programs	4,165,200	4,165,200	3,844,663	(320,537)	-8%
U.S. Citizenship & Immigration Services (USCIS)	2,870,997	3,054,829	2,906,866	(147,963)	-5%
Federal Law Enforcement Training Center (FLETC)	282,812	282,812	276,413	(6,399)	-2%
Science & Technology Directorate (S&T)	1,006,471	1,006,471	1,176,432	169,961	17%
Domestic Nuclear Detection Office (DNDO)	383,037	383,037	331,738	(51,299)	-13%
TOTAL BUDGET AUTHORITY:	\$ 56,169,614	\$ 55,728,760	\$ 56,983,449	\$ 1,254,689	2.25%
Mandatory, Fee, and Trust Funds	(10,179,438)	\$ (9,697,347)	\$ (9,578,910)	\$ 118,437	-1.22%
Discretionary Offsetting Fees	(3,533,561)	(3,442,780)	(4,180,357)	(737,577)	21%
NET DISC. BUDGET AUTHORITY:	\$ 42,456,615	\$ 42,588,633	\$ 43,224,182	\$ 635,549	-
Less Rescission of Prior-Year Carryover - Regular Appropriations:⁴	(151,582)	(40,474)	(41,942)	-	0%
ADJUSTED NET DISC. BUDGET AUTHORITY:	\$ 42,305,033	\$ 42,548,159	\$ 43,182,240	\$ 634,081	1%
SUPPLEMENTAL:⁵	\$ 5,865,603	-	-	-	-

Figure 3.52 U.S. Department of Homeland Security, total budget authority by organization.

Homeland Security

For the 2011 budget year, there is ample support for technological innovation, including but not limited to

- Advanced imaging technology
- Portable explosive trace detection
- Radiological/nuclear detection equipment
- E-Verify increase
- Cyber-network funds
- Modernization of flood mapping
- Sensor technology
- Safecon cargo scanners

In addition to these innovations, DHS allotted a plethora of funds to new positions in canine departments, behavioral detection teams, detachment units, federal air marshals, and intelligence analysts.

The 2012 budget requests include a host of ambitious projects. True to its general trend, DHS mixes personnel with emerging technologies in hopes of fielding the most efficient practices. On the personnel front, the agency increases the use of behavior detection officers in both airports and other settings. The budget simultaneously seeks funding for 37 visual intermodal prevention and response teams (VIPR) whose task is to identify terrorists by behavior, security screening, and other methods of targeting (see Figure 3.53).

Internet Exercise: Find out about VIPR teams at https://www.youtube.com/watch?v=T_Y93bin2b0.

The 2012 budget seeks funds to bolster ranks in the historically understaffed USCG, and at the same time increase funding for marine safety programs and environmental protection and response as well as patrol vigilance in American fishing zones. The USCG will also receive funds for its severely depleted capital fleet and facilities. The budget requests increases for various technological innovations, including

- Federal network protection and the deployment of Einstein 3-Computer Protection
- BioWatch 2–3 Detection Systems
- Southwest and northern border technology



Figure 3.53 A TSA VIPR member. (www.tsa.gov.)

3.3 Budgeting, Finance, and Funding in Homeland Security

Finally, the 2012 budget appears most dedicated to workplace enforcement in the matter of immigration violations. For many years, critics of ICE urged more emphasis on businesses that employ illegals. DHS officials seem inclined to go in that direction with increased funding requests for

- Workplace enforcement
- E-Verify
- VISA security program
- Detention reform
- Funding for beds
- Secure communities

3.3.9 Budget Year: 2013

During the short history of DHS, it has been rare to discern or discover any cuts or reductions in the DHS budget. 2013 is a rare exception to that rule, though in the grand scheme of things, the reductions are minor. Figure 3.54⁵⁶ lays out the impact.

Part of the reason for reduction relates to mandatory cuts posed under various budgetary restrictions imposed by Congress, but it is fair to say that the unbridled growth of DHS has not gone unnoticed. Spending has been escalating with little restraint, and DHS has learned that money alone is not the sole solution to the security problem. For the budget year 2013, the emphasis has been, allegedly, on greater efficiencies on how funds are expended. With a \$59,000,000,000 billion budget, it is a reasonable line of scrutiny (see Figure 3.55).⁵⁷

In this budgetary cycle, the emphasis will include a reinforcement of traditional models of homeland defense as well as some significant innovation, including but not limited to these crucial missions:

- Preventing terrorism and enhancing security
- Securing and managing our borders
- Enforcing and administering our immigration laws
- Safeguarding and securing cyberspace
- Ensuring resilience to disasters⁵⁸

A host of new programmatic designs and initiatives were launched and supported during this budget year. In the transportation sector, especially in relation to air travel, the TSA PreCheck

	FY 2011 Enacted ¹	FY 2012 Enacted ²	FY 2013 Pres. Budget	FY 2013 +/- FY 2012
	\$000	\$000	\$000	\$000
Net Discretionary:	\$ 42,206,179	\$ 46,248,145	\$ 44,942,110	\$ (1,306,035)
Discretionary Fees:	3,442,780	3,547,405	3,756,720	209,315
<i>Less rescission of prior year funds: ³</i>	<i>(524,185)</i>	<i>(200,736)</i>	-	<i>200,736</i>
Gross Discretionary	45,124,774	49,594,814	48,698,830	(895,984)
Mandatory, Fee, Trust Funds:	9,682,503	10,118,541	10,333,516	214,975
Total Budget Authority:	\$ 54,807,277	\$ 59,713,355	\$ 59,032,346	\$ (681,009)
Supplemental: ⁴	\$ -	\$ -	\$ -	\$ -
<i>Less rescission of prior year supplemental funds:</i>	<i>\$ -</i>	<i>\$ -</i>	<i>\$ -</i>	<i>\$ -</i>

Figure 3.54 Fiscal year 2013 overview.

Homeland Security

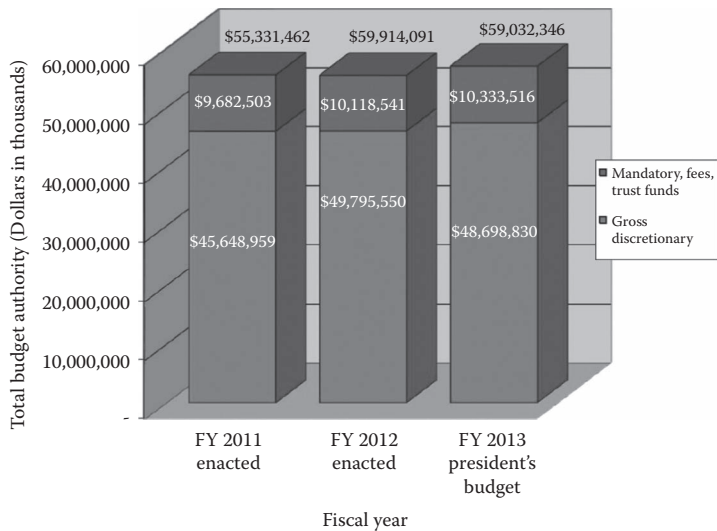


Figure 3.55 Total budget authority in thousands of dollars.



Figure 3.56 TSA PreCheck program logo.

program was expanded and assessed in order that more travelers might avoid the headaches of long security lines (see Figure 3.56).

Based on the Israeli model, TSA has been increasing its human observation program of ferreting out suspected terrorists by observational techniques by and through its Screening of Passengers through Observation Techniques (SPOT) program. Some signs worth noting are shown in Figure 3.57.

Like many TSA programs, the intentions do not always lead to desired, or acceptable, results. After spending nearly \$1 billion on the program, the General Accounting Office, by audit, indicates the results are mixed and that further investment may be unwise.⁵⁹

Other highlights of the budget year include these undertakings:

- Implementation of the National Terrorism Advisory System to replace the historic color-coded model
- Increased funding for fusion centers and joint terrorism task forces
- Enhanced cargo security screening programs
- Increased Border Patrol personnel
- Launched E-Verify Self-Check program to allow easier decision-making on the part of foreign workers to enter the country or not

The 2013 budget year also witnessed increased recognition of cyber threats and cybercrime as a means or methods of terror as well as the need to enhance border security. In the latter case,



Figure 3.57 Signs of a possible security risk.

the funding has shown little effectiveness in limiting the unceasing wave of illegals crossing the American frontier.

3.3.10 Budget Year: 2014

For the 2014 budgetary cycle, the amount allotted to DHS again remains somewhat static, though the sum could not ever be construed as paltry. While there is a small decline in the overall budget of nearly \$60,000,000,000 billion, that portion has little impact on the day-to-day operations of this agency. The question is not whether the department has sufficient funding, but whether its funding is being used wisely and intelligently. Part of that determination is how the pie is sliced from the original budget granted—for in evaluating where the money goes, one discerns DHS’s priorities by its trail of expenditures and spending. In 2014, the funds were parsed up by various percentages as is evident in Figure 3.58.⁶⁰

Stresses on efficiency and wise use of taxpayer funding continue in this budget year. DHS willingly indicates a desire to remove duplicative processes; to sell and alienate real property

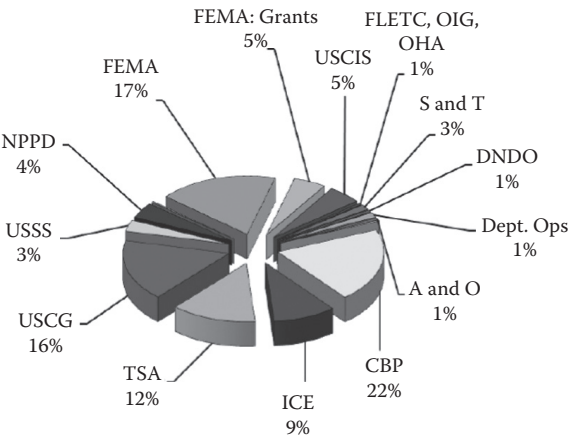


Figure 3.58 Total budget authority by organization.

Homeland Security

that does not advance the mission of the agency; and to find “commonalities” in the various processes it undertakes such as in investigations, travel and conferences, vetting and screening techniques, and hiring and staffing practices. DHS also concludes that its impact, aside from security, is economic by the many services provided and constituencies served.

In general terms, the department continues its mission orientation in light of the budget and how those mission goals and objectives are achieved by the disbursement of those special funds. In this budget year, certain priorities emerge especially as relates to the cyber world and its global impact. Other highlights in the cycle include

- Preboard aviation vetting program that identifies and prevents known threat parties from ever boarding a plane
- Increased funding for VIPR teams working in public transit
- Development and strategic placement of equipment and technology that targets radiological threats
- Funding for a National Bio and Agro-Defense Facility in the state of Kansas (see Figure 3.59)
- Increased aircraft resource for customs and border patrol
- Recapitalization of the aging USCG fleet
- Substantial funding to U.S. computer emergency readiness teams
- Consolidation of diverse grant programs into a central office

The 2014 DHS budget confronts, willingly or not, the turmoil and tumult caused by a porous and insecure border. Admitting that its immigration system “is broken and outdated,”⁶¹ DHS has clearly failed to allay the natural fears of a nation on edge from an unchecked influx of illegals. And while there is a more liberal tolerance for not checking admittees to this country, nor dealing with those here illegally for political reasons, the citizenry clearly pays a price in matters of security and domestic tranquility. Undeniably, the immigration system mirrors the chaos of our current political climate. DHS has committed express funds, in substantial numbers, to deal with the immigration issue. Some examples are



Figure 3.59 National Bio and Agro-Defense Facility, Manhattan, Kansas.

3.3 Budgeting, Finance, and Funding in Homeland Security

- *Law enforcement officers*—The FY 2014 budget supports 21,370 CBP Border Patrol agents and a record 25,252 CBPOs who work with federal, state, and local law enforcement.
- *Increase to CBPO staffing level*: \$210.1M—CBP requests an increase of \$210.1 million to fund 1,600 additional CBPOs, to include 70 canine teams at ports of entry (POEs) and 245 mission and operational support positions, equating to 1,845 positions.
- *Trusted Traveler programs (composed of NEXUS, SENTRI, FAST, and Global Entry)*—The Trusted Traveler programs continue to expand and included more than 1.5 million members in FY 2012.
- *Integrated fixed towers*: \$77.4M (0 FTE)—An increase of \$77.4 million is requested to support the deployment of proven, effective surveillance technology along the highest trafficked areas of the southwest border in Arizona.
- *King Air (KA)-350CER multi-role enforcement aircraft (MEA)*: \$43.0M (0 FTE)—The budget requests an increase of \$43 million for two KA-350CER MEA.
- *Tactical communication (TACCOM)*: \$40.0M (0 FTE)—The FY 2014 request includes \$40 million for the development and deployment of CBP's land mobile radio TACCOM systems.
- *Tethered Aerostat Radar System (TARS)*: \$37.4M (0 FTE)—The TARS program is a multi-mission capability that supports the counter-narcotics, air surveillance, and U.S. air sovereignty missions.
- *Targeting systems*: \$31.6M (0 FTE)—The requested increase of \$31.6 million will support enhancements to targeting systems by updating rules in real time and providing CBP with 24/7 targeting capability.
- *ATS operations and maintenance (O&M)*: \$31.1M (0 FTE)—The request of \$31.1 million maintains current service levels and ensures sustained operations and performance of ATS and subsystems, addresses resource requirements that will support the maintenance of and enhancements and improvements to ATS, and supports the overall O&M of the six modules that comprise ATS.
- *P-3 Service Life Extension program (SLEP)*: \$24.0M (0 FTE)—The budget requests \$24 million for the P-3 SLEP.
- *Consolidation of the NTC*: \$13.2M (0 FTE)—The requested \$13.2 million will fund the initial cost of consolidating CBP's NTCs for passengers and cargo into one location.
- *CBP Mobile program*: \$10.8M (0 FTE)—CBP requests an increase of \$10.8 million for 1,500 additional mobile devices, which include electronic link mobile operations (ELMO) devices, handheld license plate/document readers (MC75A), and secure electronic enrollment kits (SEEK).
- *Integrated traveler processing*: \$8.0M (0 FTE)—CBP requests an increase of \$8 million for investing in technology to improve processing at air and land POEs through the acquisition of 60 kiosks at airports and at eight high-volume pedestrian crossings.
- *NTC—enhanced targeting*: \$7.8M (0 FTE)—The requested increase of \$7.8 million will allow CBP to continue to support significant workload increases and program expansion.
- *Sensor upgrades for tactical aircraft*: \$3.5M (0 FTE)—The budget requests \$3.5 million for tactical aircraft sensor upgrades.
- *Marine vessels*: \$3.5M (0 FTE)—The budget requests \$3.5 million for marine vessels.
- *Single Transaction Bond Centralization*: \$3.3M (0 FTE)—The request includes \$3.3 million for the Single Transaction Bond Centralization initiative.⁶²

Homeland Security

Internet Exercise: For the full text of the appropriations act, which authorizes funds for DHS, see <https://www.congress.gov/bill/113th-congress/house-bill/2217>.

3.3.11 Budget Year: 2015

Funding for the 2015 budget cycle is slightly higher than the previous 3 years of allotments, but this increase has only been in small sums when compared with the rate of government growth and expenditure (see Figure 3.60).⁶³

DHS Secretary, Jeh Johnson, refers to the amount as “historic” when it comes to the investment in people needed to carry out the diverse functions of the department.⁶⁴ More interestingly, the budgetary analysis displays a new and heightened sensitivity concerning the relationship of effective practice and expenditure—this being a matter of first instance in the budgetary process. In other words, DHS is now not simply demanding funds for its endless array of responsibilities but is also asking whether the funds have been intelligently and effectively expended considering specific results. The 2015 budget begins that new approach with a look at TSA—an agency that has brought significant negative press, and embarrassment, to DHS. TSA agents have been caught stealing property during searches, taking and selling imagery from full-body scans, and even been indicted on charges of using their positions to smuggle drugs. This in addition to subjecting children and the elderly—apart from the general population—to what have been argued are over-the-top screening practices. Despite recent relaxing of some screening policies, and as a result of past improprieties, the 2015 budget manifests a novel mentality of questioning whether or not there is a better way to conduct business—not only for TSA but for other arms of DHS as well. Thus, when DHS indicates that it must align

Gross Discretionary, Mandatory, Fees, and Trust Funds

	FY 2013 Revised Enacted ¹	FY 2014 Enacted ²	FY 2015 Pres. Budget ³	FY 2015 +/- FY 2014	FY 2015 +/- FY 2014
	\$000	\$000	\$000	\$000	%
Departmental Operations⁴	\$ 708,695	\$ 728,269	\$ 748,024	\$ 19,755	2.7%
Analysis and Operations (A&O)	301,853	300,490	302,268	1,778	0.6%
Office of the Inspector General (OIG)	137,910	139,437	145,457	6,020	4.3%
U.S. Customs & Border Protection (CBP)	11,736,990	12,445,616	12,764,835	319,219	2.6%
U.S. Immigration & Customs Enforcement (ICE)	5,627,660	5,614,361	5,359,065	(255,296)	-4.5%
Transportation Security Administration (TSA)	7,193,757	7,364,510	7,305,098	(59,412)	-0.8%
U.S. Coast Guard (USCG)	9,972,425	10,214,999	9,796,995	(418,004)	-4.1%
U.S. Secret Service (USSS)	1,808,313	1,840,272	1,895,905	55,633	3.0%
National Protection and Programs Directorate (NPPD)	2,638,634	2,813,213	2,857,666	44,453	1.6%
Office of Health Affairs (OHA)	126,324	126,763	125,767	(996)	-0.8%
Federal Emergency Management Agency (FEMA)	11,865,196	11,553,899	12,496,517	942,618	8.2%
FEMA: Grant Programs	2,373,540	2,530,000	2,225,469	(304,531)	-12.0%
U.S. Citizenship & Immigration Services (USCIS)	3,378,348	3,219,142	3,259,885	40,743	1.3%
Federal Law Enforcement Training Center (FLETC)	243,111	258,730	259,595	865	0.3%
Science & Technology Directorate (S&T)	794,227	1,220,212	1,071,818	(148,394)	-12.2%
Domestic Nuclear Detection Office (DNDO)	302,981	285,255	304,423	19,168	6.7%
TOTAL BUDGET AUTHORITY:	\$ 59,209,964	\$ 60,655,168	\$ 60,918,787	\$ 263,619	0.4%
Less: Mandatory, Fee, and Trust Funds:	(11,308,307)	(11,526,210)	(11,890,496)	(364,286)	3.2%
GROSS DISC. BUDGET AUTHORITY:	47,901,657	49,128,958	49,028,291	(100,667)	-0.2%
Less: Discretionary Offsetting Fees:	(3,553,282)	(3,733,428)	(4,414,798)	(681,370)	18.3%
NET DISC. BUDGET AUTHORITY:	\$ 44,348,375	\$ 45,395,530	\$ 44,613,493	\$ (782,037)	-1.7%
Less: FEMA Disaster Relief - Major Disasters Cap Adjustment:	\$ (6,075,554)	\$ (5,626,386)	\$ (6,437,793)	\$ (811,407)	14.4%
Less: Rescission of Prior-Year Carryover - Regular Appropriations: ⁵	(151,463)	(543,968)	-	543,968	-100.0%
ADJUSTED NET DISC. BUDGET AUTHORITY:	\$ 38,121,358	\$ 39,225,176	\$ 38,175,700	\$ (1,049,476)	-2.7%
Supplemental:⁶	\$ 11,483,313	-	-	-	-

Figure 3.60 Total budget authority by organization.

3.3 Budgeting, Finance, and Funding in Homeland Security

“passenger screening resources based on risk,”⁶⁵ the conclusion demonstrates a desire to correlate expenditure with sensible practices—a philosophical outlook long overdue at the agency. As a result, TSA is now investing more in

- TSA PreCheck, which eliminates a portion of those known to be safe bets from the screening process
- Increasing preflight watch list analysis in its Secure Flight program, which targets those more likely to be security problems
- Expending more funds on the screening of bags for explosives, ensuring 100% compliance since mechanical processes are always more efficient than human interaction

The 2015 budget also witnesses increased funding for both capital and operations for the USCG—likely the most efficient and well-run agency in the entire DHS. Aside from updating its cutter fleet and replacing old and aging equipment, the USCG continues to receive funding based on exceptional performance. Some examples include

- Increased funding for aircraft and air vessels dedicated to first-responder activity
- Enhanced funding for offshore boarding and interdiction for ships before port entry
- Funding for additional vessel board and search teams (VBSTs)

Other evidence that DHS is trying to correlate expenditures with efficient operations include

- ICE’s determination that paper-based worker verifications system can be replaced with electronic methods
- Creation of an E-Verify Self-Check system, which is computer based at lower cost
- Priority funding for computer-based cybersecurity capable of tracking cybercrime and other offenses, which ICE can employ to discover patterns of identity theft and other computer-based frauds
- Increased cybersecurity funding for the U.S. Secret Service, who must be vigilant in both physical and cyberspace

Finally, the 2015 budget delivered a new category of funding, designated “opportunity funding.”⁶⁶ At this level of budget, DHS identifies “climate change” as being a variable that is crucial to FEMA planners and first responders. While some may argue the science is settled as to climate change, it is a fair conclusion that the agreement on what to do about climate change is anything but universal.

Over the last decade, the inevitable march of bureaucratic growth and budgetary increase unfolds. While there may be less funding, temporarily, to go around, DHS maintains its bureaucratic perpetuity by the myriad of functions and tasks that have been entrusted to it. The only forces that appear to chink its armor have been budgetary restrictions, which Congress bemoans but lacks the will and tenacity to enforce; and the increased role of private-sector partners, who have demonstrated greater efficiencies and dedication to consumer and customer service.

3.3.12 Budget Year: 2016

During the 2016 budgetary cycle, the DHS funding priorities reflect both tradition and new directions. The funding is affirmed and correlated to the mission of the DHS in five areas:

- prevent terrorism and enhance security
- secure and manage our borders
- enforce and administer our immigration laws

Homeland Security

- safeguard and secure cyberspace
- strengthen national preparedness and resilience.

While the 2016 budget witnessed generally across the board increases, greater sums were allotted to successful initiatives. The Trusted Traveler Programs were further buttressed because it represented a means and method to expend less energy on those already verified and more energy on those that should be suspect in the airport security environment as well as the cross border commercial traveler such as truckers. Easier access between Canada and Mexico is one of the chief aims of the Trusted Traveler program. Figure 3.61⁶⁷ highlights the various Trusted Traveler programs.

\$373.5 million in funding for new border surveillance technology is also provided.

The 2016 budgetary cycle attends to a human and public relations nightmare—unaccompanied children making border crossings separate from their nuclear family or other caregiver. The budget provides funds for the costs associated with apprehension and care of up to 104,000 unaccompanied children, in preparing the temporary holding of these children at the Rio Grande Detention Facility (Figure 3.62).⁶⁸

Internet Exercise: Find out where the detention centers are located at: <https://www.ice.gov/detention-facilities>

In the area of cybersecurity, DHS exhibits strong awareness on how threats to our cyber-structure are equally disabling than our physical infrastructure. The budget for 2016 issues vastly increased funding for network maintenance and security as well as protection against malicious attacks across governmental systems. The budget supports Einstein 3—a cyber-defense system that not only detects malicious traffic by intrusion prevention capabilities for Internet Service Providers.

Finally, as a matter of first instance, the budget, issued under President Obama, correlates the dynamic of climate change to homeland defense and parses out funding to discover the correlation between climate change and the FEMA side of natural disaster and emergency.

While some people laud the move, others have discouraged the “politicization” of DHS citing climate change as a secondary or peripheral factor. Recent disasters and evidence increasingly show climate change to be a very immediate and growing threat.⁶⁹

For a summary of the 2016 Budget, see Figure 3.63.⁷⁰

 Departures from U.S. Airports \$85 USD  Travel by Air Eligibility U.S. citizens and U.S. lawful permanent residents	 Entry into the U.S. from International Destinations \$100 USD  Travel by Air, Land and Sea includes TSA Pre✓ Eligibility U.S. citizens, U.S. lawful permanent residents, and select foreign nationals	 Entry into the U.S. from Canada \$50 USD  Travel by Air, Land and Sea may include TSA Pre✓ Eligibility U.S. citizens, U.S. lawful permanent residents, Canadian citizens, Canadian permanent residents, and Mexican nationals	 Entry into the U.S. from Canada and Mexico \$122.50 USD  Travel by Air and Land may include TSA Pre✓ Eligibility U.S. citizens, U.S. lawful permanent residents and all foreign nationals.	 For truck drivers entering and exiting the U.S. from Canada and Mexico \$50 USD  Travel for Commercial Trucks does not include TSA Pre✓ Eligibility U.S. citizens, U.S. lawful permanent residents, Canadian citizens, Canadian permanent residents, and Mexican nationals
--	--	--	---	---

Figure 3.61 Summaries and highlights from the Trusted Traveler programs.

3.3 Budgeting, Finance, and Funding in Homeland Security



Figure 3.62 The Rio Grande Detention Facility has not been without its share of controversy.

Total Budget Authority by Organization Gross Discretionary, Mandatory, Fees, and Trust Funds

	FY 2014 Revised Enacted	FY 2015 Pres. Budget	FY 2016 Pres. Budget	FY 2016 +/- FY 2015	FY 2016 +/- FY 2015
	\$000	\$000	\$000	\$000	%
Departmental Management and Operations (DMO)	\$ 728,269	\$ 748,024	\$ 960,627	\$ 212,603	28.4%
Analysis and Operations (A&O)	300,490	302,268	269,090	(33,178)	-11.0%
Office of the Inspector General (OIG)	139,437	145,457	166,284	20,827	14.3%
U.S. Customs & Border Protection (CBP)	12,463,893	12,764,835	13,565,294	800,459	6.3%
U.S. Immigration & Customs Enforcement (ICE)	5,948,161	5,359,065	6,281,637	922,572	17.2%
Transportation Security Administration (TSA)	7,420,517	7,305,098	7,346,924	41,826	0.6%
U.S. Coast Guard (USCG)	10,098,753	9,810,468	9,963,914	153,446	1.6%
U.S. Secret Service (USSS)	1,845,272	1,895,905	2,204,122	308,217	16.3%
National Protection and Programs Directorate (NPPD)	2,810,413	2,857,666	3,102,862	245,196	8.6%
Office of Health Affairs (OHA)	126,763	125,767	124,069	(1,698)	-1.4%
Federal Emergency Management Agency (FEMA)	10,869,247	12,179,177	13,235,589	1,056,412	8.7%
FEMA: Grant Programs	2,530,000	2,225,469	2,231,424	5,955	0.3%
U.S. Citizenship & Immigration Services (USCIS)	3,368,805	3,770,026	4,003,638	233,612	6.2%
Federal Law Enforcement Training Center (FLETC)	258,730	259,595	266,694	7,099	2.7%
Science & Technology Directorate (S&T)	1,220,212	1,071,818	778,988	(292,830)	-27.3%
Domestic Nuclear Detection Office (DNDO)	288,055	304,423	357,327	52,904	17.4%
TOTAL BUDGET AUTHORITY:	\$ 60,417,017	\$ 61,125,061	\$ 64,858,484	\$ 3,733,423	6.1%
Less: Mandatory, Fee, and Trust Funds:	(10,826,987)	(11,987,538)	(12,909,477)	(921,939)	7.7%
GROSS DISC. BUDGET AUTHORITY:	49,590,030	49,137,523	51,949,007	2,811,484	5.7%
Less: Discretionary Offsetting Fees:	(3,526,605)	(4,505,990)	(4,042,340)	463,650	-10.3%
NET DISC. BUDGET AUTHORITY:	\$ 46,063,425	\$ 44,631,533	\$ 47,906,667	\$ 3,275,134	7.3%
Less: FEMA Disaster Relief - Major Disasters Cap Adjustment:	\$ (5,626,386)	\$ (6,437,793)	\$ (6,712,953)	\$ (275,160)	4.3%
Less: Rescission of Prior-Year Carryover - Regular Appropriations:	(543,968)			-	
ADJUSTED NET DISC. BUDGET AUTHORITY:	\$ 39,893,071	\$ 38,193,740	\$ 41,193,714	\$ 2,999,974	7.9%

Figure 3.63 The 2016 DHS Budget by organization.

Homeland Security

3.3.13 Budget Year: 2017

With the election of President Donald J. Trump, DHS focused on enforcement, criminal apprehension, Border Patrol and ICE purposes. Even so, throughout the first 2 years of President Trump's administration, he was repeatedly criticized for his handling of families and children at the border, even though his predecessor handled this complex problem in a very similar way. By 2017, the caravans and illegal crossing rates had so risen, that the emphasis had to change. See Figure 3.64.

Because of these forces, DHS reassessed and reapplied its resources to more traditional functions. Some examples include:

- \$292.0 million for U.S. Customs and Border Protection (CBP) targeting programs, which includes support for the National Targeting Centers (NTC) for passengers and cargo.
- \$5.1 billion for the Transportation Security Administration (TSA) for transportation screening operations to ensure the freedom and movement of people and commerce.
- \$2.1 billion for ICE criminal investigators to protect the U.S. against terrorist and other criminal organizations that threaten public safety and national security.
- \$355.7 million to maintain the necessary infrastructure and technology along the Nation's borders to ensure CBP law enforcement personnel.
- \$2.0 billion for Coast Guard counter-drug and alien migration interdiction operations.
- Support for Coast Guard air and surface fleet recapitalization to include \$240 million for production of four Fast Response Cutters
- \$2.2 billion to enable U.S. Immigration and Customs Enforcement (ICE) to maintain nearly 31,000 detention beds for individuals presenting a flight risk, a risk to public safety or national security, or who are subject to mandatory detention.
- \$347 million for the Criminal Alien Program to support ICE in the apprehension and removal of both at-large and incarcerated convicted criminals. These resources include funding for an additional 100 officers to support ICE in this mission area.⁷¹

For a summary of budgetary priorities for 2017, see Figure 3.65.⁷²



Figure 3.64 Migrants looking for routes on a map of Mexico. Ciudad Deportiva Magdalena Mixhuca temporary camp, Mexico City, November 9, 2018. (This file is licensed under the Creative Commons Attribution-Share Alike 4.0 International license. https://upload.wikimedia.org/wikipedia/commons/a/ab/Caravana_Migrante_en_la_Ciudad_de_M%C3%A9xico_--_16.jpg.)

3.3 Budgeting, Finance, and Funding in Homeland Security

FY 2017 Percent of Total Budget Authority by Organization

\$66,801,948,000

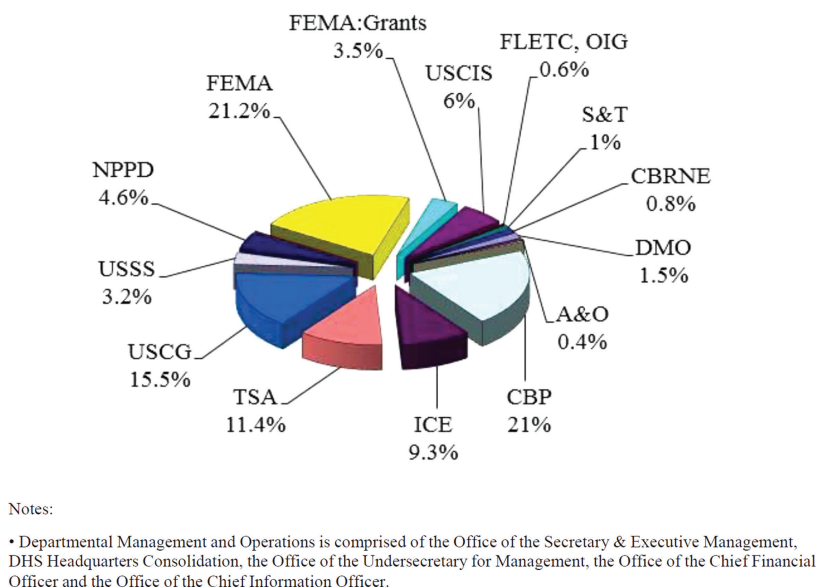


Figure 3.65 A summary of the budget priorities of 2017 as outlined by organization.

3.3.14 Budget Year: 2018

One of the most obvious shifts in budgetary priorities, aside from the return to a more law enforcement mentality noted in 2017, was the shift of funds from the overly administrative and bureaucratic offices to the operational DHS functions such as ICE, the Border Patrol and other Immigration Services. A summary of the 2018 budget's manifest cuts in the Office of the Under Secretary, the IG office, the Office of Health Affairs, and others, while redirecting those funds to the core missions of the DHS (see Figure 3.66).⁷³

While there are not many new initiatives in this budget than from the previous year, clearly, the administration and DHS itself were returning to border protection. Highlights of the budget include:

- \$3.1 billion for 43,190 Transportation Security Officers (TSOs) to maintain effective and efficient passenger screening at airport checkpoints
- \$277.2 million for acquisition of checked baggage screening technology to improve TSA's threat detection capabilities
- \$971.3 million to improve security of the U.S. cyber infrastructure in collaboration with public, private, and international partners, including \$279 million for the Continuous Diagnostics and Mitigation (CDM) program. See Figure 3.67.⁷⁴
- \$2.7 billion to fund both direct and indirect costs for 51,379 detention beds, which are comprised of 48,879 adult beds, and 2,500 family beds. Removable aliens who are apprehended and determined to need custodial supervision are placed in detention facilities.
- \$185.9 million to support the expansion of ICE's interior enforcement activities under the Executive Order to hire an additional 850 immigration officers, 150 criminal investigators, and 805 law enforcement mission support staff.

Total Budget Authority by Organization

Gross Discretionary, Mandatory, Fees, and Trust Funds

Dollars in Thousands

Organization	FY 2016 Revised Enacted ¹	FY 2017 Annualized CR	FY 2018 President's Budget	FY 2017 to FY 2018 Total Changes	FY 2018 +/- FY 2017 %
Office of the Secretary and Executive Management	\$145,332	\$133,474	\$130,307	(\$3,167)	-2.4%
Office of the Under Secretary for Management	\$937,081	\$962,133	\$768,664	(\$193,469)	-20.1%
Analysis and Operations	\$260,224	\$254,303	\$252,405	(\$1,898)	-0.7%
Office of Inspector General	\$161,467	\$137,151	\$133,974	(\$3,177)	-2.3%
U.S. Customs and Border Protection	\$13,295,208	\$13,474,495	\$16,387,729	\$2,913,234	21.6%
U.S. Immigration and Customs Enforcement	\$6,177,578	\$6,139,917	\$7,942,072	\$1,802,155	29.4%
Transportation Security Administration	\$7,543,364	\$7,425,805	\$7,582,228	\$156,423	2.1%
U.S. Coast Guard	\$10,893,631	\$10,940,660	\$10,673,010	(\$267,650)	-2.4%
U.S. Secret Service	\$2,191,808	\$2,190,481	\$2,208,626	\$18,145	0.8%
National Protection and Programs Directorate	\$3,075,838	\$3,081,428	\$3,277,489	\$196,061	6.4%
Office of Health Affairs	\$125,333	\$122,747	\$111,319	(\$11,428)	-9.3%
Federal Emergency Management Agency	\$15,712,464	\$16,151,751	\$15,552,106	(\$599,645)	-3.7%
United States Citizenship and Immigration Services	\$3,787,338	\$3,606,909	\$4,442,039	\$835,130	23.2%
Federal Law Enforcement Training Center	\$244,480	\$243,994	\$272,759	\$28,765	11.8%
Science and Technology	\$776,653	\$771,690	\$627,324	(\$144,366)	-18.7%
Domestic Nuclear Detection Office	\$347,036	\$342,059	\$330,440	(\$11,619)	-3.4%
Total Budget Authority	\$65,674,835	\$65,978,997	\$70,692,491	\$4,713,494	7.1%
Less: Mandatory, Fee, and Trust Funds	\$12,448,305	\$12,843,978	\$14,198,144	\$1,354,166	10.5%
Gross Discretionary Budget Authority	\$53,226,530	\$53,135,019	\$56,494,347	\$3,359,328	6.3%
Less: Discretionary Offsetting Fees	\$4,218,831	\$4,110,295	\$5,039,914	\$929,619	22.6%
Net Discretionary Budget Authority	\$49,007,699	\$49,024,724	\$51,454,433	\$2,429,709	5.0%
Less: FEMA Disaster Relief - Major Disasters	\$6,712,953	\$6,712,953	\$6,793,000	\$80,047	1.2%
Less: USCIS - CHIMP Funding	\$4,000	\$4,000	\$4,000	\$0	0.0%
Less: Rescissions to Prior Years Balances ²	\$1,049,217	\$1,049,217	\$593,745	(\$455,472)	-43.4%
Adjusted Net Discretionary Budget Authority	\$41,241,529	\$41,258,554	\$44,063,688	\$2,805,134	6.8%

¹ FY16 \$24M Transfer from FEMA-DRF to OIG is included in funding line² Includes Rescissions to FEMA – DRF, FEMA – DADLP, & USCG – Alteration of Bridges

Figure 3.66 The 2016 DHS Budget by organization.

- \$1.2 billion for recapitalization of USCG assets including, \$500 million for production of the first of 25 Offshore Patrol Cutters, \$240 million for production of four Fast Response Cutters, \$19 million to maintain the accelerated timeline for acquisition of a new heavy polar icebreaker, and \$52 million to missionize an HC-27J surveillance aircraft for USCG use.
- \$1.6 billion for 32 miles of new border wall construction, 28 miles of levee wall along the Rio Grande Valley, and 14 miles of new border wall system that will replace existing secondary fence in the San Diego Sector, where apprehensions are the highest along the Southwest Border, and where a border wall system will deter access to drug and alien smuggling organizations.

3.3 Budgeting, Finance, and Funding in Homeland Security

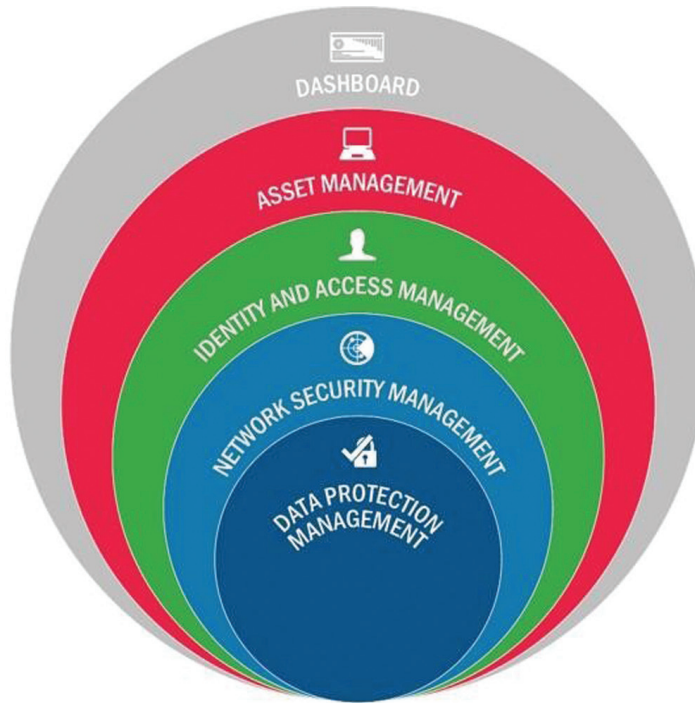


Figure 3.67 The Continuous Diagnostics and Mitigation (CDM) program priorities.

The question of border wall construction has been, to say the least, a contentious debate. At times the divide between our two political parties has been acrimonious and bitter. For Democrats, nearly in unison, there has been keen resistance to the building of any Wall while Republicans hold that the Wall assures our safety and security. The views of these political parties could not be more extreme. Democratic Senator Chuck Schumer equates the Wall debate with Trump's intent to "tear families apart" and acting in an "inhumane way." Senator Tom Cotton of Arkansas took a legal and law enforcement bent in response to Schumer stating: "If illegal aliens with final orders of removal can't be deported, who can be? Democrats have a radical, open-borders position."⁷⁵

Internet Exercise: Discover the differing styles of Wall Design at the CPB web location at: <https://www.cbp.gov/frontline/border-wall-prototype-designs>

President Trump remarked in February of 2019:

Our progress will be limited if we do not secure our porous border and put an end to the human trafficking and humanitarian crisis that is taking place at the southern border. It is indeed a crisis. And, you know, we have right now an invasion. If you look at what's going on with the caravans, it's an invasion. There are three caravans heading our way. If we had a wall, it wouldn't even be a problem. But we've sent 2,500 military down to help Border Patrol and law enforcement. And I have to say, the military has done an incredible job, including helping us with some walls and some fences, which are very nice to say.

Unsecure borders give traffickers free and clear passage to transport their victims into the United States. It's a tremendously big money-maker for some very, very bad people. In fiscal year 2018, ICE made more than 1,500 human trafficking arrests, with 97 percent of that for sex trafficking.⁷⁶

Homeland Security

3.3.15 Budget Year: 2019

2019 continues to see a rapid and very generous reinvestment in the personnel and aligned equipment and technology demands for those laboring in homeland security. The budget lays out very ambitious goals for hiring in most operational areas including border patrol, ICE and Immigration-Citizenship, screening personnel in TSA, as well as a historic reinvestment in the capital assets of the United States Coast Guard. In short, the budget mirrors the administration's desire to put people and equipment where needed to combat potential terrorist activity. A review of Figure 3.68⁷⁷ makes plain this plan.

Total Budget Authority by Organization Gross Discretionary, Mandatory, Fees, and Trust Funds

Organization	FY 2017 Enacted	FY 2018 President's Budget	FY 2019 President's Budget	FY 2018 to FY 2019 Total Changes	FY 2019 +/- FY 2018 %
Office of the Secretary and Executive Management	\$137,034	\$130,307	\$128,860	(\$1,447)	-1.1%
Management Directorate	\$673,624	\$768,664	\$1,083,318	\$314,654	+29.0%
Analysis and Operations	\$263,551	\$252,405	\$253,253	\$848	+0.3%
Office of Inspector General	\$175,000	\$133,974	\$138,369	\$4,395	+3.2%
U.S. Customs and Border Protection	\$14,439,714	\$16,327,340	\$16,690,317	\$362,977	+2.2%
U.S. Immigration and Customs Enforcement	\$6,770,344	\$7,942,072	\$8,816,586	\$874,514	+9.9%
Transportation Security Administration	\$7,771,340	\$7,582,228	\$7,726,058	\$143,830	+1.9%
U.S. Coast Guard	\$10,670,895	\$10,673,010	\$11,651,747	\$978,737	+8.4%
U.S. Secret Service	\$2,310,578	\$2,208,626	\$2,416,624	\$207,998	+8.6%
National Protection and Programs Directorate	\$3,269,850	\$3,277,489	\$3,348,261	\$70,772	+2.1%
Office of Health Affairs	\$123,548	\$111,319	-	(\$111,319)	-
Federal Emergency Management Agency	\$16,231,885	\$16,111,936	\$16,071,073	(\$40,863)	-0.3%
United States Citizenship and Immigration Services	\$4,179,364	\$4,442,039	\$4,719,570	\$277,531	+5.9%
Federal Law Enforcement Training Centers	\$242,518	\$272,759	\$382,134	\$109,375	+28.6%
Science and Technology Directorate	\$781,746	\$627,324	\$583,283	(\$44,041)	-7.6%
Domestic Nuclear Detection Office	\$352,484	\$330,440	-	(\$330,440)	-
Countering Weapons of Mass Destruction	-	-	\$429,266	\$429,266	+100.0%
Total Budget Authority	\$68,393,475	\$71,191,932	\$74,438,719	\$3,246,787	+4.4%
Less: Mandatory, Fee, and Trust Funds	\$13,491,530	\$14,747,687	\$14,724,748	(\$22,939)	-0.2%
Gross Discretionary Budget Authority¹	\$54,901,945	\$56,444,245	\$59,713,971	\$3,269,726	+5.5%
Less: Discretionary Offsetting Fees	\$4,117,976	\$4,988,963	\$5,235,504	\$246,541	+4.7%
Discretionary Budget Authority	\$50,783,969	\$51,455,282	\$54,478,467	\$3,023,185	+5.6%
Less: FEMA Disaster Relief - Major Disasters	\$6,713,000	\$6,793,000	\$6,652,000	(\$141,000)	-2.1%
Less: USCIS - CHIMP Funding	\$4,000	\$4,000	\$4,000	-	-
Less: USCG - OCO Funding	\$162,692	-	-	-	-
Less: Rescissions to Prior Years Balances	(\$1,483,667)	(\$593,400)	(\$300,000)	\$293,400	-97.8%
Adjusted Net Discretionary Budget Authority	\$42,420,610	\$44,064,882	\$47,522,467	\$3,457,585	+7.3%

¹FY 2017 Gross Discretionary includes USCG - OCO Funding.

Figure 3.68 The 2019 DHS Budget by organization.

3.3 Budgeting, Finance, and Funding in Homeland Security

Other noted investments are quite evident in the U.S. Secret Service, the Customs function of ICE and Border Patrol, and additionally, dramatically increased funding for FLETC—the training agency responsible for many of these new employees.

Other budgetary highlights for 2019 include:

- \$1.6 billion for 65 miles of new border wall construction in the Rio Grande Valley Sector.
- \$210.5 million to support the recruitment, hiring, and training of 750 additional Border Patrol Agents (BPAs). This is part of a multi-year initiative to hire a total of 5,000 additional BPAs as directed by Presidential Executive Order 13767 Border Security and Immigration Enforcement Improvements.
- \$570.9 million for an additional 2,000 law enforcement officers and 1,312 support personnel to process the greater workload that results from enhanced enforcement efforts.
- \$511.1 million for transportation costs associated with the transfer and removal of illegal immigrants
- \$1.9 billion for the recapitalization of USCG assets including but not limited to \$750.0 million to continue efforts to design and construct the Nation's first new heavy Polar Icebreaker in over 40 years.
- \$3.2 billion funds an additional 687 screeners for a total of 43,877 Transportation Security Officers (TSOs), the highest level in history.
- \$1.4 billion to support an additional 450 Secret Service agents, officers, and professional staff, for a total of 7,600 positions by the end of FY 2019.
- \$73.9 million for acquisition and operation of computed tomography (CT) systems for use at high-risk airports.

See Figure 3.69.⁷⁸

Computer Tomography—commonly referred to as the CT scanner—is increasingly a TSA tool at local airports. As of 2020, the following airports had installed CT scanners.

- Hartsfield-Jackson Atlanta International Airport (ATL)
- Baltimore-Washington International Airport (BWI)
- Chicago O'Hare International Airport (ORD)
- Cincinnati/Northern Kentucky International Airport (CVG)
- Detroit Metropolitan Wayne County Airport (DTW)
- Houston Hobby Airport (HOU)



Figure 3.69 Computer tomography (CT) systems.

Homeland Security

- Indianapolis International Airport (IND)
- John F. Kennedy International Airport (JFK)
- Logan International Airport (BOS)
- Los Angeles International Airport (LAX)
- Miami International Airport (MIA)
- Oakland International Airport (OAK)
- Phoenix Sky Harbor International Airport (PHX)
- Ronald Reagan Washington National Airport (DCA)
- St. Louis Lambert International Airport (STL)
- Tampa International Airport (TPA)
- Washington-Dulles International Airport (IAD)

3.3.16 Budget Year: 2020

As DHS nears its 20th anniversary, the budgetary analysis, from 2002 forward, manifests some interesting trends and movements in the priorities of the department. While earlier budgets were mostly enamored with TSA and critical infrastructure such as airports and government facilities, the evolution of the budgetary process mirrors the priorities of a given time and administration. What is clear in 2020 is the centrality of the border in our homeland defense. What is undeniable in 2020 is how the nation's virtual infrastructure and the many challenges of cybersecurity weigh prominently in budget decisions. Finally, what also continually courses its way through the budget are the search and implementation of technological systems and solutions—finding ways to drive costs down with less use of human capital and more aggressive use of unmanned technology. The revolution in drones, robotic instruments, and nuclear and biohazard technology systems, to name just a few, takes over an increasing amount of human activity. As the billions of funds are annually spent, the decision makers are under increasing pressure to economize and assess the efficacy of their strategy. As DHS strategically plans its future and weighs protocols and stratagems, it always makes sense to evaluate how things are working, especially given the major taxpayer investment. For example, our border continues to press our patience and sensibility. Yet, a longitudinal view makes plain that there is success and failure that is often surprising. Our nation's Southwest border apprehensions are significantly higher, year-on-year, in 2019, so it is debatable whether the Trump administration, CPB and DHS, and its technological investments had paid off. See Figure 3.70⁷⁹ for the downward trend in border apprehensions.

For 2020, the thrust of the budgetary process continued to reflect current security challenges and to anticipate future threats. Some of the highlights were:

- \$163.6 million to support the hiring, training, and equipping of 750 additional Border Patrol Agents (BPAs)
- \$5.0 billion for construction of approximately 200 miles of a new border wall system.
- \$313.9 million for an additional 1,000 law enforcement officers and 666 support personnel. This request provides additional law enforcement capacity to strengthen immigration enforcement.
- \$694.1 million for federal network protection, which includes Continuous Diagnostics and Mitigations (CDM) and National Cybersecurity Protection System (NCPS).
- \$79.7 million funds an additional 700 screeners, for a total of 44,577 Transportation Security Officers (TSOs), the highest level in history.

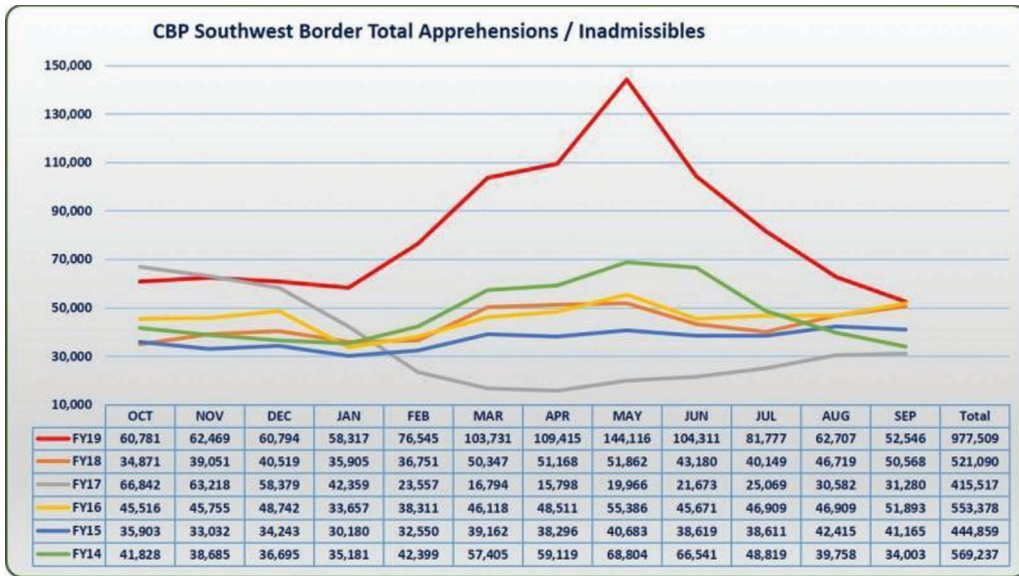


Figure 3.70 Recent trends in border apprehensions as reported by U.S. Customs and Boarder Protection.

See Figure 3.71.⁸⁰

In general, the 2020 budget year continues to reflect the crucial priorities of DHS but puts its stress on personnel, human capital, and the equipment and tools necessary for success in the field. Gone from the budget are climate change and other global initiatives.

DHS's 2021 budget can be accessed here:

https://www.dhs.gov/sites/default/files/publications/fy_2021_dhs_bib_web_version.pdf

Under current President Biden, it is clear that, as per prior administrations, the emphasis, funding, and focus with continue to change and more closely align with—and reflect—the key objectives of the administration's agenda.

3.4 Conclusion

Exactly how DHS was established, shaped, and foundationally organized receives significant attention in this chapter. DHS arises from both political and security influences, though it could not be erected until a legal framework had been established. The various executive orders and legislative enactments that lead to DHS are fully analyzed. In addition, aligned legislation that impacts how DHS conducts its business, such as the USA Patriot Act, presently the U.S. Freedom Act of 2015, is fully covered. Specialized subject-matter legislation is given a broad overview, including the REAL ID program, the US-VISIT, now the Office of Biometric Identity Management, regulations and the entity renamed the Office of Biometric Identity Management, the SAFETY Act, and the laws governing registration of select industries.

The chapter also delves into the budget and finance aspects of DHS. In particular, the chapter traces the budgetary history of DHS and correlates budgetary allotments to mission decisions. Hence, budget years 2002–2021 evidence both consistency and adaptability in how budgets are calculated. Basic homeland functions remain a constant in every budget, though the rise of technology funds in the delivery of homeland services has surely seen growth. The budgetary analysis also features new initiatives that require an infusion of funds, especially

FY 2020 Percent of Total Budget Authority by Organization
\$92,077,529

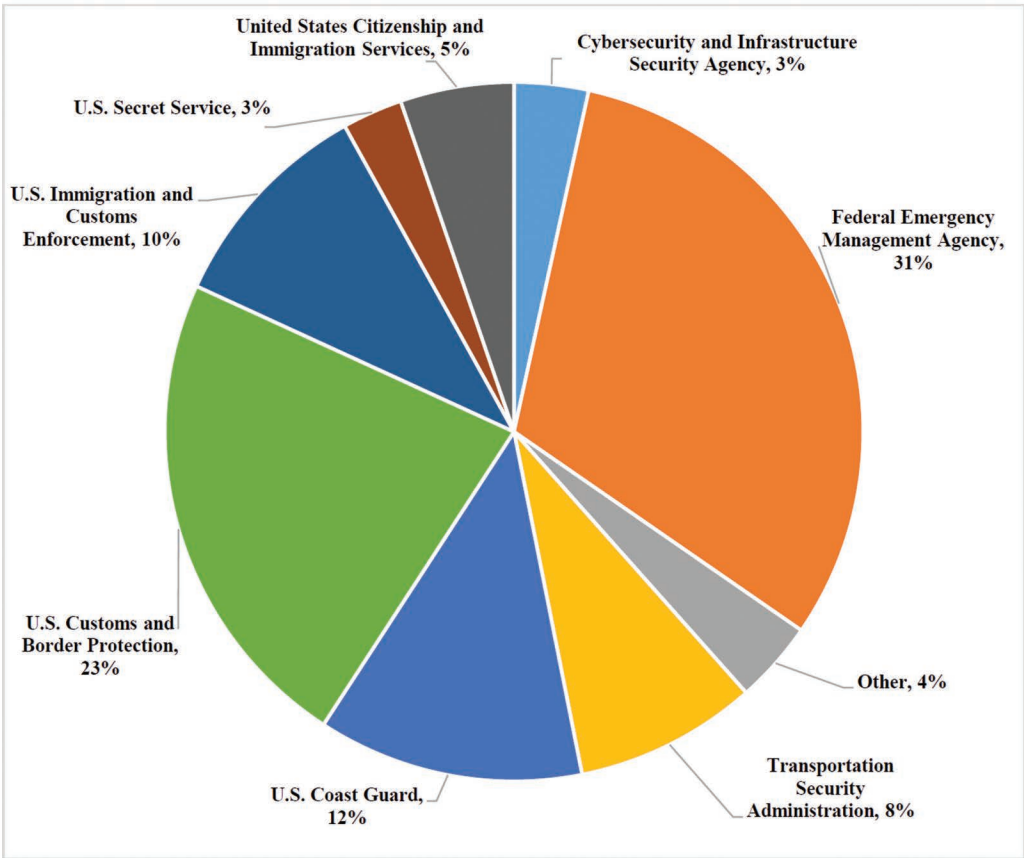


Figure 3.71 The 2020 DHS Budget by organization.

as to cybersecurity, the construction and erection of a Wall, border patrol, and physical assets dedicated to such, and major capital investments in the long-neglected USCG fleet. While the budget history of DHS has many constants and predictable line items, change is often driven by new technologies, innovative software and hardware programs dedicated to particular industries as well as by the endless array of new security challenges that have become part of the American landscape.

Keywords

Allotments; Best PracticesBiometrics; Budgeting; Cabinet; CBP Targeting Systems; Container Security Initiative; Core Values; Customs-Trade Partnership Against Terrorism; Cybersecurity; Domestic Nuclear Detection Office; Emergency Alert System; Executive Branch; Executive Order; Exigent Circumstances; Federal Communications Commission; Finance; Jurisdiction; Laws; Legal Authority; Legislation; National Biodefense Analysis and Countermeasure Center; National Incident Management System; National Preparedness Integration program; Office of

Management and Budget; Passive Radiation Detection; Posse Comitatus Act; Private Sector Justice; Privatization; Project BioShield; Radiation Detection Monitors; Radiography; REAL ID Program; Regulations; Rescue 21; SAFETY Act; SBInet; Secure Border Initiative; Secure Flight System; Spectroscopic Portal; USA Patriot Act; USNORTHCOM or NORTHCOM; US-VISIT

Discussion Questions

1. Explain how the DHS of today differs from the DHS of 2003.
2. Critics of the early acts and executive orders relating to the establishment of DHS often say that these promulgations suffered from a lack of vision and thinking. Can you make this argument in any meaningful way?
3. The USA Patriot Act has received blistering critiques from civil libertarians. Why? Do you concur?
4. Why do early executive orders and legislation so firmly emphasize the role of infrastructure?
5. In the assessment of budget histories, point out two trends over the life of DHS.
6. In the assessment of the DHS budget, are there any shortcomings or oversights? Lay out precise examples.
7. Discuss two recent initiatives involving global trade and DHS.
8. If you had to predict, will future budgets of DHS be increased or decreased in the next decade?

Practical Exercises

1. Visit www.whitehouse.gov. Find and summarize three recent executive orders relating to homeland security.
2. Assess and evaluate recent amendments to the Homeland Security Act of 2002. List four major categories of adaptation and adjustment in the act since 2002.
3. Compare and contrast the original USA Patriot Act with the provisions enacted in 2008. Some have argued that the later act lacks teeth and rigor. Is there any truth to this assertion? Provide proof by the language of the acts.
4. Prepare a form file for the Office of Biometric Identity Management program.
5. Review the budgetary cycle of DHS over the period 2003–2015. Identify four major trends in the allotment of funds. Evaluate whether budgetary cycles are influenced by trends and pressures to target specialized activities.

Notes

- 1 Federal Register, Friday, December 3, 2010, 75(232), Proclamation 8607, 75613.
- 2 Executive Order, Improving Critical Infrastructure Cybersecurity, February 12, 2013.
- 3 Presidential Proclamation, Critical Infrastructure Security and Resilience Month, 2015, October 29, 2015.

Homeland Security

- 4 Federal Register, Tuesday, January 27, 2009, Executive Order 13493, 74 FR 4901, <https://federalregister.gov/a/E9-1895> (accessed August 9, 2020).
- 5 American Civil Liberties Union, President Obama issues executive order institutionalizing indefinite detention, March 7, 2011, <http://www.aclu.org/national-security/president-obama-issues-executive-order-institutionalizing-indefinite-detention> (accessed August 9, 2020).
- 6 See: Executive Order, Protecting America Through Lawful Detention of Terrorists, January 30, 2018, <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-protecting-america-lawful-detention-terrorists/> (accessed August 9, 2020).
- 7 See: Executive Order 13846, Reimposing Certain Sanctions with Respect to Iran, August 6, 2018, <https://www.federalregister.gov/documents/2018/08/07/2018-17068/reimposing-certain-sanctions-with-respect-to-iran/> (accessed August 9, 2020).
- 8 See the Inspector General’s Report on FISA warrant abuse at: US Department of Justice, Office of Inspector General, Review of Four FISA Applications and Other Aspects of the FBI’s Crossfire Hurricane Investigation (December 2019), <https://oig.justice.gov/reports/2019/o20012.pdf> (accessed August 9, 2020).
- 9 Homeland Security Act of 2002. Public Law 107-296, November 25, 2002, http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (accessed August 9, 2020).
- 10 President’s Remarks at Homeland Security Bill Signing. Department of Homeland Security Official Home Page, November 25, 2002, <https://georgewbush-whitehouse.archives.gov/news/releases/2002/11/20021125-6.html> (accessed August 9, 2020).
- 11 J. David, The Defense of North America: NORAD & NORTHCOM, *Canada-United States Law Journal*, 29 (2003): 261.
- 12 NORAD and USNORTHCOM Public Affairs, USNORTHCOM Hurricane Sandy Response Support, November 7, 2012, <http://www.northcom.mil/Newsroom/tabid/3104/Article/563649/usnorthcom-hurricane-sandy-response-support-nov-7.aspx> (accessed August 9, 2020).
- 13 C. Khalil, Thinking intelligently about intelligence: A model global framework protecting privacy, *George Washington International Law Review*, 47 (2015): 919; A. Deeks, An international legal framework for surveillance, *Virginia Journal of International Law*, 55 (2015): 219.
- 14 See K. L. Hermann, Reviewing Bush-era counter-terrorism policy after 9/11: Reconciling ethical and practical considerations, *Homeland Security Review*, 4 (2010): 139; See also C. L. Richardson, The creation of judicial compromise: Prosecuting detainees in a National Security Court System in Guantanamo Bay, Cuba, *Homeland Security Review*, 4 (2010): 119.
- 15 U.S. Department of Homeland Security, *Fact Sheet: The USA Patriot Act—A Proven Homeland Security Tool* (12/14/050).
- 16 C. Savage, “Deal reached on extension of Patriot Act,” *New York Times*, May 19, 2011.
- 17 Republican Study Committee, *Legislative Bulletin*, May 26, 2011.
- 18 See U.S. Patriot Act, section 215 (2011).
- 19 USA Freedom Act of 2015, Public Law No: 114-23, June 2, 2015.
- 20 Ibid.
- 21 For a full text of a recent legislative bill, yet to be authorized, see: H.R.6172 - USA FREEDOM Reauthorization Act of 2020, 116th Congress (2019–2020), <https://www.congress.gov/bill/116th-congress/house-bill/6172/text> (accessed August 9, 2020).
- 22 See: R. Lucas, Scathing Report Puts Secret FISA Court into the Spotlight. Will Congress Act? NPR.com, December 22, 2019, <https://www.npr.org/2019/12/22/790281142/scathing-report-puts-secret-fisa-court-into-the-spotlight-will-congress-act> (accessed August 9, 2020); See also: Senate RPC Website, RISA Reauthorization page, <https://www.rpc.senate.gov/policy-papers/fisa-reauthorization> (accessed August 9, 2020).
- 23 See: US Foreign Intelligence Surveillance Court website, Current Membership page, <https://www.fisc.uscourts.gov/current-membership> (accessed August 9, 2020).
- 24 REAL ID Act of 2005, P.L. 109-13, *U.S. Statutes at Large*, 119 (2005): 231, <http://www.govtrack.us/congress/bill.xpd?tab=summary&bill=h109-418> (accessed August 9, 2020).
- 25 Department of Homeland Security, Office of Inspector General, Potentially high costs and insufficient grant funds pose a challenge to REAL ID implementation, 1 (OIG-09-36) (March 2009).
- 26 Center for Immigration Studies, REAL ID implementation: Less expensive, doable, and helpful in reducing fraud (January 2011), <http://cis.org/real-id> (accessed August 9, 2020).

- 27 US Department of Homeland Security Website, REAL ID page, <https://www.dhs.gov/real-id> (accessed August 9, 2020).
- 28 Center for Immigration Studies, REAL ID implementation: Less expensive, doable, and helpful in reducing fraud (January 2011), <http://cis.org/real-id> (accessed August 9, 2020); J. Hatch, Requiring a nexus to national security: Immigration, “terrorist activities,” and statutory reform, *Brigham Young University Law Review*, 2014 (2014): 697, <http://digitalcommons.law.byu.edu/lawreview/vol2014/iss3/10> (accessed August 9, 2020).
- 29 Department of Homeland Security, Office of Inspector General, Potentially high costs and insufficient grant funds pose a challenge to REAL ID implementation, 6 (OIG-09-36) (March 2009).
- 30 J. Hatch, Requiring a nexus to national security: Immigration, “terrorist activities,” and statutory reform, *Brigham Young University Law Review*, 2014 (2014): 697, <http://digitalcommons.law.byu.edu/lawreview/vol2014/iss3/10> (accessed August 9, 2020); G. D. Kravitz, REAL ID: The devil you don’t know, *Harvard Law and Policy Review*, 3 (2009): 431.
- 31 J. Harper, Florida’s implementation of the federal Real ID Act of 2005, (February 24, 2011), <https://www.cato.org/publications/congressional-testimony/floridas-implementation-federal-real-id-act-2005> (accessed August 9, 2020).
- 32 Office of Biometric Identity Management Expenditure Plan, Fiscal Year 2015 Report to Congress, (June 11, 2015).
- 33 *Ibid.*, 14–16.
- 34 Homeland Security Appropriations Act of 2007, P.L. 109–295, Section 550, *U.S. Statutes at Large*, 120 (2006): 1355.
- 35 For a complete list of chemicals subject to the administrative regulations, see Code of Federal Regulations, title 6, part 27 (2007), https://www.dhs.gov/xlibrary/assets/chemsec_appendixafinal-rule.pdf (accessed August 9, 2020).
- 36 Code of Federal Regulations, title 6, sec. 25.7(j) (2004).
- 37 M. Paddock, Homeland Security funding since 9/11, *Homeland Security Today* (September 2011): 9.
- 38 Congressional Budget Office, Economic and issue brief: Federal funding for Homeland Security (April 30, 2004): 5, http://www.cbo.gov/ftpdocs/54xx/doc5414/homeland_security.pdf (accessed August 9, 2020).
- 39 National Biodefense Analysis and Countermeasures Center (NBACC) Fact Sheet, https://www.dhs.gov/sites/default/files/publications/national_biodefense_analysis_and_countermeasures_center-nbacc-12132019.pdf (accessed August 9, 2020).
- 40 U.S. Department of Homeland Security, *Sample National Terrorism Advisory System Alert*, http://www.dhs.gov/sites/default/files/publications/ntas-sample-alert_0_0.pdf (accessed August 9, 2020).
- 41 Department of Homeland Security, *Budget in Brief: Fiscal Year 2005* (Washington, DC: U.S. Government Printing Office, 2005), 12, http://www.dhs.gov/sites/default/files/publications/FY_2005_BIB_4.pdf (accessed August 9, 2020).
- 42 Department of Homeland Security, *Performance Budget Overview FY 2005* (Washington, DC: U.S. Government Printing Office, 2005), 8, http://www.dhs.gov/xlibrary/assets/2004PBO_FINAL_29_JAN_04.pdf (accessed August 9, 2020).
- 43 Department of Homeland Security, *Budget-in-Brief: Fiscal Year 2006* (Washington, DC: U.S. Government Printing Office, 2006), 16, http://www.dhs.gov/xlibrary/assets/Budget_BIB-FY2006.pdf (accessed August 9, 2020).
- 44 General Dynamics, *Rescue 21: Saving Lives for the 21st Century*, C4 Systems, Section 21.1, http://gacc.nifc.gov/eacc/dispatch_centers/ILC/Mobilization_Guide/Chapter%2020%202011.pdf (accessed August 9, 2020).
- 45 J. Edwards, U.S. Coast Guard taking a Coast Guard mission to new heights, *Military.com*, February 23, 2007.
- 46 For a full analysis of various detection systems, see A. Glaser, *Detection of Special Nuclear Materials* (Princeton University, April 16, 2007), http://www.princeton.edu/~aglasers/lecture2007_detection.pdf (accessed August 9, 2020).
- 47 S. Rosière and R. Jones, Teichopolitics: Re-considering globalization through the role of walls and fences, *Geopolitics*, 17 (2012): 217; C. Amuedo-Dorantes and S. Pozo, On the intended and unintended consequences of enhanced U.S. border and interior immigration enforcement: Evidence from Mexican deportees, *Demography*, 51 (2014): 2255.

Homeland Security

- 48 Department of Homeland Security, *Budget-in-Brief: FY 2008* (Washington, DC: U.S. Government Printing Office, 2008), 15, http://www.dhs.gov/xlibrary/assets/budget_bib-fy2008.pdf (accessed August 9, 2020).
- 49 The USA's SBInet Border Security Project, *Defense Industry Daily*, <http://www.defenseindustrydaily.com/21b-sbinet-border-security-contract-goes-to-team-boeing-02648/> (accessed August 9, 2020); A. Lipowicz, Boeing's SBInet contract gets the axe (January 14, 2011), <https://washingtontechnology.com/articles/2011/01/14/dhs-cancels-rest-of-sbinet-and-plans-mix-of-new-technologies-at-border.aspx> (accessed August 9, 2020).
- 50 Implementation and Coordination of TSA's Secure Flight Program (July 2012), https://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf (accessed August 9, 2020).
- 51 M. Paddock, Cuts affect more than just the bottom line, *Homeland Security Today*, June (2011): 9.
- 52 See Executive Order: Reducing Improper Payments and Eliminating Waste in Federal Programs, November 23, 2009.
- 53 Memorandum from DHS Secretary Janet Napolitano to C. K. Edwards Acting Inspector General, Council of Inspectors General on Integrity and Efficiency, *Quarterly High-Dollar Overpayments Report for the period October to December 2011*, February 22, 2012, <http://www.dhs.gov/xlibrary/assets/mgmt/cfo-high-dollar-overpayments-october-december-2011.pdf> (accessed August 9, 2020).
- 54 U.S. Department of Homeland Security, *Budget-in-Brief, Fiscal Year 2012*, 17 (2011).
- 55 *Ibid.*, 21.
- 56 Department of Homeland Security, *2013 Budget in Brief*, 3 (2013), <http://www.dhs.gov/xlibrary/assets/mgmt/dhs-budget-in-brief-fy2013.pdf> (accessed August 9, 2020).
- 57 *Ibid.*, 21.
- 58 *Ibid.*, 8–9.
- 59 GAO Report, *TSA Should Limit Future Funding for Behavior Detection Activities* GAO-14-159 (November 2013), <http://www.gao.gov/assets/660/658923.pdf> (accessed August 9, 2020).
- 60 Department of Homeland Security, *2014 Budget in Brief*, 5 (2014), <https://www.dhs.gov/sites/default/files/publications/FY%202014%20BIB%20-%20FINAL%20-508%20Formatted%20%284%29.pdf> (accessed August 9, 2020).
- 61 *Ibid.*, 8.
- 62 *Ibid.*, 114–117.
- 63 Department of Homeland Security, *2015 Budget in Brief*, 7 (2015), <http://www.dhs.gov/publication/fy-2015-budget-brief> (accessed August 9, 2020).
- 64 *Ibid.*, 9.
- 65 *Ibid.*, 10.
- 66 *Ibid.*, 14.
- 67 US Department of Homeland Security Website, Trusted Traveler Programs page, <https://ttp.dhs.gov/> (accessed August 9, 2020).
- 68 US Department of Homeland Security website, US Immigration and Customs Enforcement, Detention Facilities page: Rio Grande Detention Center, <https://www.ice.gov/detention-facility/rio-grande-detention-center> (accessed August 9, 2020).
- 69 See: Department of Homeland Security, 2016 Strategic Sustainability Performance Plan (June 2016), https://www.dhs.gov/sites/default/files/publications/SSPP%20DHS%202016%20SSPP%20FINAL%20REVISED%20090116%20508%20COMPLIANT_0.pdf (accessed August 9, 2020).
- 70 US Department of Homeland Security, *Budget in Brief Fiscal Year 2016*, 10 (2016), https://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf (accessed August 9, 2020).
- 71 See: US Department of Homeland Security, *Budget in Brief Fiscal Year 2017*, (2017), https://www.dhs.gov/sites/default/files/publications/FY2017_BIB-MASTER.pdf (accessed August 9, 2020).
- 72 See: US Department of Homeland Security, *Budget in Brief Fiscal Year 2017*, 9 (2017), https://www.dhs.gov/sites/default/files/publications/FY2017_BIB-MASTER.pdf (accessed August 9, 2020).
- 73 US Department of Homeland Security, *Budget in Brief Fiscal Year 2018*, 11 (2018), <https://www.dhs.gov/sites/default/files/publications/DHS%20FY18%20BIB%20Final.pdf> (accessed August 9, 2020).
- 74 See: US CISA website, Continuous Diagnostics and Mitigation page, <https://www.us-cert.gov/cdm/home> (accessed August 9, 2020).

- 75 Both conversations come from a Twitter debate at: Jason Hopkins, “Senator Tom Cotton Fires Back at Fellow Senator Chuck Schumer: ‘Democrats Have a Radical, Open-Borders Position,’” *The Minnesota Sun*, June 24, 2019, <https://theminnesotasun.com/2019/06/24/senator-tom-cotton-fires-back-at-fellow-senator-chuck-schumer-democrats-have-a-radical-open-borders-position/> (accessed August 9, 2020).
- 76 Remarks by President Trump in Meeting on Human Trafficking on the Southern Border, February 1, 2019, <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-meeting-human-trafficking-southern-border> (accessed August 9, 2020).
- 77 US Department of Homeland Security, *Budget in Brief Fiscal Year 2019*, 11 (2019), <https://www.dhs.gov/sites/default/files/publications/DHS%20BIB%202019.pdf> (accessed August 9, 2020).
- 78 Ibid.
- 79 See: US Department of Homeland Security, US Customs and Border Protection Website, Southwest Border Migration FY2019 total apprehensions, <https://www.cbp.gov/newsroom/stats/sw-border-migration/fy-2019> (accessed August 9, 2020).
- 80 US Department of Homeland Security, *Budget in Brief Fiscal Year 2020*, 7 (2020), https://www.dhs.gov/sites/default/files/publications/fy_2020_dhs_bib.pdf (accessed August 9, 2020).



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

4

Risk Management, Threats, and Hazards

OBJECTIVES

1. To define the standard and best practices used in risk management in the world of homeland security
2. To describe the process of basic risk assessment and the CARVER+Shock assessment tool
3. To distinguish between threats and hazards and describe how they are analyzed and rated in risk assessment
4. To define the various categories of weapons of mass destruction (WMD), including nuclear, chemical, biological, and nerve agents
5. To differentiate between specific nuclear and radiological WMD and biological and chemical agents, such as anthrax, sarin, and ricin; their delivery methods; and their effects
6. To comprehend the importance of the country's information infrastructure and its vulnerability to an attack and identify the steps taken to secure it
7. To recognize the various government agencies involved in the cybersecurity of the United States and outline their mission and responsibilities
8. To illustrate the various public-private partnerships in homeland security and analyze their effectiveness

4.1 Introduction

The fundamental thrust of homeland security, dealing with risk, threats, and hazards, and how to prepare, respond, and recover from their effects, encompasses this chapter. In other words, how does government operate in the world of risk and threat and simultaneously provide for a secure homeland? What means and methods for prediction, mitigation, and recovery in the matter of risk are the most suitable? What types of plans and planning seem to work best in the world of homeland security? How does the governmental entity prepare and train for such

Homeland Security

events? This chapter delves into standard as well as best practices in the defense of a nation. First, it will consider the idea of threat, its scope and definition, its types and categories, and the distinction between the natural and man-made varieties. Second, the coverage will include an analysis of risk theory—that body of thought that teaches operatives how to identify risk, how to assess its impact, and how to track its influence. In addition to risk and threat, the chapter will evaluate the most efficacious means of planning and preparedness. It could be no truer than an ounce of prevention is worth a pound of cure in the world of homeland security. How one prepares for tragedy has much to do with success or failure in response and recovery. How one trains and educates the homeland security professional can be just as telling. Finally, this section will evaluate how agencies and their operatives need to communicate so that homeland security protocol achieves its ultimate end—that of safety and security for the community.

4.2 Risk Management

The work of homeland security delves into the nature of risk, whether at airports or busways, public courthouses, or national monuments. Risk constitutes what might happen or what is likely to happen given a certain set of circumstances. Risk is what can go wrong. A risk is what the homeowner takes when he or she does not evacuate when told to get out of the path of a hurricane. Risk is what air travelers are willing to tolerate in a system that lacks security checkpoints. Risk is what the country will tolerate when no mechanisms exist to check visitors at the border. In a word, risk is something each person lives with each day, from driving in a car to cycling across the hinterlands. Yet, some risks are more preventable and less serious than others. In evaluating risk, one must look to not only the nature of any risk but also to its consequences in both an individual and collective sense. Some refer to this formula in an equational sense¹—as a series of risk constituents. The risk is calculated relative to the harm the hazard causes and the level and magnitude of exposure to the said harm. The formula might look like this:

$$\text{Risk} = \text{Hazard} \times \text{Exposure} \quad (4.1)$$

Hazard is the mechanism that causes the harm, and exposure is the extent, depth, and breadth of the risk as influenced by the nature of the hazard. Thus, if anthrax is plugged into the risk equation, it is a small chore to conclude that anthrax constitutes the type of risk the individual and the collective should avoid. In a policy context, therefore, it makes perfect sense for governments to marshal resources to attack this risk—more so than an avalanche of candy bars from an upended truck. Herein lies the rub—to weigh and factor the risk considering harm and its scope. Some risks are high and others lower, and some “risks” pose no risk at all. To be sure, terrorism is high up on the list of potential harm that homeland specialists must prepare for. And risk will be geographically variable, country by country and place to place. “Terrorism has many faces and countless are the possibilities of implementing an attack against American interests under the umbrella of terrorism.”² The risk manager must anticipate every imaginable version of terrorist act to properly prepare for it.

Looked at from a different perch, risk relies on probability analysis.

4.2.1 The Nature of Risk

Risk is not an easy concept to fully define for it has both actual and anticipatory qualities. On the one hand, all one can do is predict or anticipate what might happen yet on the other, experience dictates the reality of risk. For example, will the risk injure a human? Is it likely that this risk will be in the form of a weapon? Will the risk, if by terror motive, be individually or collectively coordinated? The risk evaluator must consider that terrorist risks are increasingly of the “lone wolf” variety, where the actor acts on his or her own although it is impossible to separate the

actor from some greater cause or aim. For example, the jihadi movement calls upon individual actors to wreak havoc on others, as part of the terrorist cause. A recent intelligence intercept was forwarded to law enforcement and other interested parties to see how this individual mindset becomes so motivated. Soldiers for the terrorist cause are urged in the following way:

Do not let this battle pass you by wherever you may be. You must strike the soldiers, patrons, and troops of the tawaghit. Strike their police, security, and intelligence members, as well as their treacherous agents. Destroy their beds. Embitter their lives for them and busy them with themselves. If you can kill a disbelieving American or European – especially the spiteful and filthy French – or an Australian, or a Canadian, or any other disbeliever from the disbelievers waging war...against the Islamic State...If you are not able to find an IED or a bullet, then single out the disbelieving American, Frenchman, or any other of their allies. Smash his head with a rock, or slaughter him with a knife, or run him over with your car, or throw him down from a high place, or choke him, or poison him...If you are unable to do so, then burn his home, car, or business. Or destroy his crops...³

Any party entrusted with risk assessment and predictive reactions must anticipate the means and methods of those inflicting risk. Other questions abound. Is there a trend afoot for more terrorist plots to be launched outside of home countries and to focus on our actual homeland? Early after 9/11, the boldness of coming to America by radical Islamists shocked the intelligence community since most of the activity up until those events were mostly stationed in the home country. In this way, risk shifts based on place or locus.⁴

Is there a correlation between some religious practice and an act of terror? Is there a specific day, holiday, or anniversary—such as the September 11, 2012, Benghazi consulate attack—where terrorist events are more apt to occur? If a chemical industry fails to secure a certain substance, what are the health ramifications? One could endlessly go on about the nature of risk and its various types. To be sure, the concept is forever evolving. The Federal Emergency Management Agency (FEMA) makes a valiant effort to quantify the process. FEMA employs probability theory when making judgments about risk. In short, risk is the probability that something will occur with an evaluation of consequence⁵ (see Figure 4.1).

The Department of Homeland Security (DHS) defines the nature of risk by three principal variables: *threat*, or the likelihood of a type of attack that might be attempted; *vulnerability*, or the likelihood that an attacker would succeed with a particular attack method; and *consequence*, or the potential impact, individually or collectively, of a particular attack. In this context, one deals in generalities rather than specifics. Sound risk reasoning demands that a measure or modality of quantification be employed when making policy about risk. In other words, can risk be quantified in some way? FEMA thinks so by evaluating some specific variable relative to the nature of the risk⁶ (see Figure 4.2).

Here, the evaluator of risk moves beyond the definition seeking to formalize the precise nature and attributes of risk. What is this risk worth? How much, in terms of assets will it destroy? What level, in a global sense, of seriousness does this risk pose? How much is at stake?

Risk is a combination of:

- The probability that an event will occur, and
- The consequences of its occurrence

	Low Risk	Medium Risk	High Risk
Risk Factors Total	1–60	61–175	≥176
Risk = Asset Value x Threat Rating x Vulnerability Rating			

Figure 4.1 Definition of risk table.

Risk assessment

Determine asset value

Determine threat rating value

Determine vulnerability rating value

Determine relative risk for each threat against each asset

Figure 4.2 Quantifying risk.

Table 4.1 Critical Infrastructure				
Infrastructure	Cyber Attack	Armed Attack (Single Gunman)	Vehicle Bomb	CBR Attack
Site	48	80	108	72
Asset value	4	4	4	4
Threat rating	4	4	3	2
Vulnerability	3	5	9	9
Structural systems	48	128	192	144
Asset value	8	8	8	8
Threat rating	3	4	3	2
Vulnerability rating	2	4	8	9

When, compared with other assets, is it worth our dedication to thwart all risks? For homeland security, the thrust will be toward quantification—using distinct variables with assigned point values to type the risk. The DHS risk formula would look something like this:

Risk = Asset value × threat rating × vulnerability rating

(4.2)

The severity of a risk will be assessed considering its value, the nature of the threat itself, and the potential for harm and injury. So, as is evident in Table 4.1, infrastructure damage is heavily weighted yet variably dependent on the method employed to inflict the damage and harm.⁷

So, this leads to the matter of risk assessment in particular terms. How do our homeland professionals and policy makers decide that this risk is worth more than another? Can they devise a meaningful system of quantification that reliably measures the effect and consequence of a risk gone wrong?

4.2.2 Risk Assessment

There are diverse ways in which risk can be measured. The Rand Organization suggests three methodologies of risk assessment⁸:

- *Analytic*: An analytic process must address all three factors that determine terrorism risk—threat, vulnerability, and consequences.
- *Deliberative*: A deliberative process is necessary because the notion of a cold, actuarial terrorism risk assessment is unrealistic. Values and judgment are part and parcel of the process and require transparency and a comprehensive public discussion of outcomes.
- *Practical*: Finally, risk assessment must be practical, which means that data collection and management requirements must be technically and economically feasible.

If DHS has any preference, it would be analytic, though it would be short-sighted to avoid the other modalities. DHS posits new, interesting variables into its risk assessment formula primarily in two ways: the value of asset and the impact on geography. In both instances, the more value, the more coverage; and the greater the impact on the populace, the higher the event will place in tabulations. At first glance, it may seem arbitrary, although nothing in the soft sciences can ever lay claim to the certitude of the hard sciences. What is so strikingly evident is that DHS is willing to place a value on these two things. In a sense, it is about as good as it can be in the imperfect world of risk assessment.

As for value, the DHS risk assessment model highlights the most notable of the targets a terrorist might choose—chemical plants, stadiums, and commercial airports. DHS then analyzes the vulnerability of each asset type relative to each attack method and the plausibility of the chosen attack method.

Additionally, DHS computes the consequential costs of a successful attack and its impact on the value of assets, the health of the collective, our economic system, and the military, and its overall psychological impact on the national psyche. This analysis yields a relative risk estimate for each asset type, applied to a given geographic area and based on the number of each asset type present within that area. DHS lists those assets that carry higher values in its equation in Figure 4.3.⁹

The risk assessment formula is then tested geographically. The geographically based approach weighs the value of assets in that particular region. Geographic regions are weighted in accordance with their area listings¹⁰ (see Figure 4.4).

Risk can also be plotted on a global scale, country by county, region by region. Identifying risks in this way aids those engaged in commerce and trade, innovation, and investment and assists in the determination of what country can be considered either a friend or foe (see Figure 4.5).¹¹

In light of this valuation, DHS computes the threat level and police and law enforcement activity relative to threats, as well as intelligence from customs and immigration and other suspicious incident data. Then, DHS considers vulnerability factors for each geographic area, such as the area's proximity to international borders and the potential for international incident. Lastly, DHS estimates the potential consequences of an attack on that area, including human health, size of population, economic conditions, military complex, and overall business and industry. DHS charts its methodology in Figure 4.6.¹²

On a narrower front, the task of risk assessment can be departmentally and programmatically driven. For example, risk for FEMA may be distinctively different from the risks of concern to immigration and citizenship. Each agency and department need to perceive risk in light of its

- | | |
|--|--------------------------------------|
| • Chemical manufacturing facilities | • Natural gas compressor stations |
| • City road bridges | • Non-power nuclear reactors |
| • Colleges and universities | • Nuclear power plants |
| • Commercial airports | • Nuclear research labs |
| • Commercial overnight shipping facilities | • Petroleum pumping stations |
| • Convention centers | • Petroleum refineries |
| • Dams | • Petroleum storage tanks |
| • Electricity generation facilities | • Potable water treatment facilities |
| • Electricity substations | • Primary and secondary schools |
| • Enclosed shopping malls | • Railroad bridges |
| • Ferry terminals—buildings | • Railroad passenger stations |
| • Financial facilities | • Railroad tunnels |
| • Hospitals | • Road commuter tunnels |
| • Hotel casinos | • Road interstate bridges |
| • Levees | • Road interstate tunnels |
| • Liquefied natural gas (LNG) terminals | • Stadiums |
| • Maritime port facilities | • Tall commercial buildings |
| • Mass transit commuter rail and subway stations | • Telcomm-telephone hotels |
| • National health stockpile sites | • Theme parks |
| • National monuments and icons | • Trans-oceanic cable landings |

Figure 4.3 High-value assets as determined by DHS.

Homeland Security

- Defense industrial base facilities
- Federal Bureau of Investigation (FBI) basic and special cases
- Gross domestic product (GDP)
- I-94 visitors from countries of interest
- Intelligence community credible and less credible threat reports
- Immigration and customs enforcement (ICE) basic and special cases
- Miles of international border
- Military bases
- Nuclear waste isolation pilot plan (WIPP) transportation routes
- Population
- Population density
- Port of entry/border crossings (people from countries of interest and annual throughput)
- Ratio of law enforcement to population
- Special events
- State international export trade
- State total agriculture sales
- Sum of population density of urban areas in state
- Sum of population of urban areas in state
- Suspicious incidents (credible and less credible)

Figure 4.4 High-value geographic target regions.

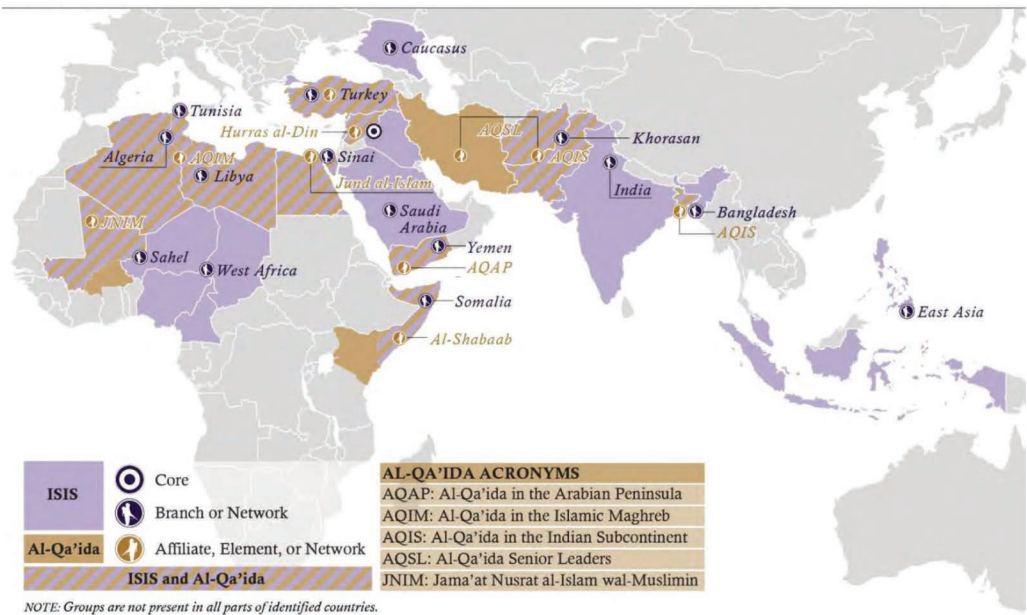


Figure 4.5 A map of ISIS, al-Qaeda, and their affiliates.

overall mission. One of the more telling illustrations can be discovered in the workings of the Federal Protective Service (FPS), which is entrusted with the protection of nearly 9,000 federal facilities. Risk assessment is central to its overall task and mission. Therefore, the FPS has developed a Risk Assessment and Management Program (RAMP), which aids FPS officers carrying out facility assessment plans.

RAMP is a risk assessment tool that is multitasked and multivariate in approach. RAMP's intent is to

- Assess and analyze the risk posed to federal facilities from terrorism, crime, natural hazards, and other serious incidents
- Centrally store, access, and report risk assessment findings, including historical information from previous assessments and other documentation

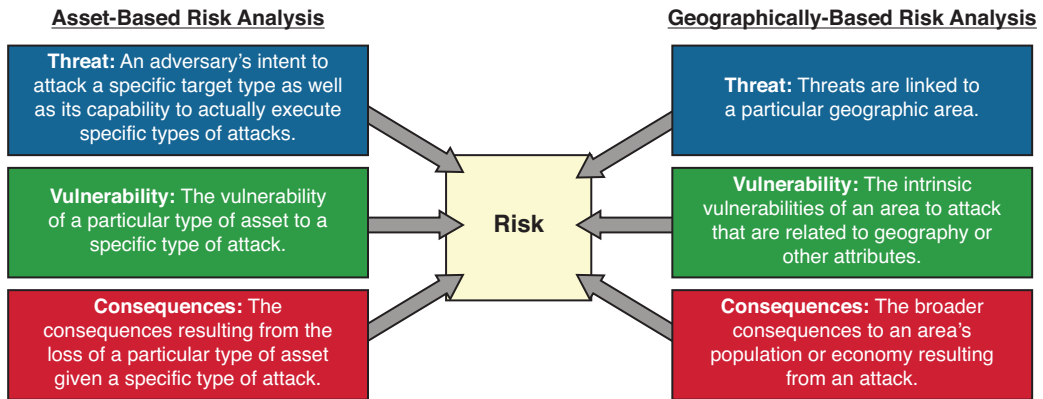


Figure 4.6 Asset-based risk analysis vs. geographically based risk analysis methodology comparison.

- Manage all aspects of the formal safety assessment (FSA) process
- Manage security post inspections, contracts, and individual guard certification compliance
- Recommend and track the implementation of countermeasures throughout their life cycle
- Perform inventory-wide analysis of the risks posed to federal facilities and the means of reducing them
- Automate and track countermeasure recommendations, implementation status, and life-cycle replacement schedules
- Track financial information for countermeasures throughout their life cycle
- Provide Occupancy Emergency Plan information, call-back lists, and so on
- Provide security access to tools and information, including a comprehensive help file
- Generate and route letters, reports, presentations, and statistical analyses and perform other administrative functions
- Provide a comprehensive comparison across the entire general services administration (GSA) inventory that FPS protects

RAMP has taken serious recent critiques over its lack of efficiency, corruption in the ranks, and an overall programmatic ineptitude that has been critiqued by the political establishment. So troublesome was the performance and cost overruns that Congress asked the inspector general (IG) to review the program. The IG essentially confirmed what Congress and select officials had already concluded: that RAMP has yet to meet its stated goals and suffers structurally from poor management and corrupt oversight. Hence, RAMP continues to remain on hold as a DHS initiative.

Internet Exercise: Read the IG report on RAMP at https://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-67_Aug12.pdf.

Whatever approach is taken with risk assessment, it is critical to gather information, anticipate events and incidents, understand the value of assets and potential harm, and weigh and contrast the functionality and importance of geographic territory.¹³ FEMA lists the potential incidents, and plugging into the formula is what is required in Table 4.2.

Internet Exercise: The National Infrastructure Simulation and Analysis Center (NISAC) conducts modeling, simulation, and analysis of the nation's critical infrastructure. NISAC

Table 4.2 Possible Hazards and Emergencies Risk Abatement

	Hazards	
Possible Hazards and Emergencies	Hazards Risk Level (None, Low, Moderate, or High)	How Can I Reduce my Risk?
Natural Hazards		
1. Floods		
2. Hurricanes		
3. Thunderstorms and lightning		
4. Tornadoes		
5. Winter storms and extreme cold		
6. Extreme heat		
7. Earthquakes		
8. Volcanoes		
9. Landslides and debris flow		
10. Tsunamis		
11. Fires		
12. Wildfires		
Technological Hazards		
1. Hazardous materials incidents		
2. Nuclear power plants		
Terrorism		
1. Explosions		
2. Biological threats		
3. Chemical threats		
4. Nuclear blasts		
5. Radiological dispersion device (RDD)		

analysts assess critical infrastructure risk, vulnerability, interdependencies, and event consequences. Visit the website at <https://www.dhs.gov/about-national-infrastructure-simulation-and-analysis-center> and familiarize yourself with the activities.

We should not ignore the capability to mitigate potential harm. Every event can be influenced in some way, whether it is the movement of people or the protection of property. Every risk can be addressed in some fashion. Government has choices in the matter to some extent. Hazard mitigation planning is the process of determining how to reduce or eliminate the loss of life and property damage resulting from natural and human-caused hazards. Figure 4.7¹⁴ charts the four-step process of mitigation.



Figure 4.7 Four-step mitigation process.

4.2.3 CARVER+Shock Assessment Tool

How assessments are carried out invariably depends on the subject matter. In the area of food supply, water, and consumables, risk evaluators have come to depend on the CARVER+Shock assessment methodology. The CARVER system employs various criteria labeled as CARVER; CARVER is an acronym for the following six attributes used to evaluate the attractiveness of a target for attack:

- *Criticality*—Measure of public health and economic impacts of an attack
- *Accessibility*—Ability to physically access and egress from target
- *Recuperability*—Ability of system to recover from an attack
- *Vulnerability*—Ease of accomplishing attack
- *Effect*—Amount of direct loss from an attack as measured by loss in production
- *Recognizability*—Ease of identifying target

In addition, the modified CARVER tool evaluates a seventh attribute, the combined health, economic and psychological impacts of an attack, or the shock attributes of a target.

The CARVER system attempts to quantify risk by assigning specific numbers for specific conditions. It looks to products and food, facilities, and manufacturing processes. So valued is its methodology that the U.S. Food and Drug Administration (FDA) has developed and disseminated software that is downloadable on the web. CARVER+Shock software requires the user to build a process flow diagram for the system to be evaluated and to answer a series of questions for each of the seven CARVER+Shock attributes for each process flow diagram node. Flow processes can be shaped and designed in a host of applications. The CARVER program employs an icon system that correlates to a specific industry or business application. Table 4.3 is a sample listing of the flow process possibilities.¹⁵

Table 4.3 CARVER+Shock Flow Process Possibilities			
Icon	Category	Subcategory	Description
Acid	Materials	Processed ingredients	A water-soluble chemical compound with a pH of less than 7 when dissolved; has a sour taste
Air dryer	Processing	Drying	Device that dries product by direct contact with heated air
Aircraft	Transportation/distribution		Using an aircraft for the transportation of materials from one location to another
Aseptic packager	Packaging		Equipment that places and seals product in a sterile container/package
Auger tank	Processing	Processing tanks	Enclosure for a large mechanical screw that mixes and moves material/product
Bags	Packaging	Packaging materials	A container of flexible material (paper, plastic, etc.) used for packaging
Bakery	Retail food service		Location where products such as bread, cake, and pastries are baked
Balance tank	Processing	Processing tanks	Used to balance the pH of a discharge so it is within certain parameters

(Continued)

Table 4.3 (Continued) CARVER+Shock Flow Process Possibilities

Icon	Category	Subcategory	Description
Barge	Transportation/ distribution		Transportation of materials along a body of water from one location to another
Batch tank	Storage	Storage tanks	A mixing/storage tank large enough for a single batch of product
Batterer	Processing	Other processing	A machine used to mix or beat a material
Bin/tub	Storage	Other storage	A large open storage vessel
Blancher	Processing	Cooking	Equipment that uses water or steam to parboil or scald material/product to remove skin or stop enzymatic action
Blast freezer	Processing	Chilling	Device that quickly freezes materials or products as they move along a conveyor using a controlled stream of cold air; generally used when small pieces need to be kept separate as they freeze, such as cut-up vegetables
Blend tank	Processing	Processing tanks	A tank used to blend/mix materials
Blender	Processing	Mixing	Mechanical mixer for chopping, mixing, or liquefying materials
Blower	Conveyance		A machine, such as a fan, that produces an air current to move materials
Bottle cleaner	Cleaning/ washing		A process to clean, wash, and sterilize bottles
Bottle hopper	Packaging		Provides a continuous flow of containers to be loaded on a conveyor
Bottler	Packaging		Automated equipment for filling bottles
Bottles	Packaging	Packaging materials	Containers with a narrow neck and no handles that can be plugged, corked, or capped
Boxes	Packaging	Packaging materials	Container with four sides and a lid or cover used for storage or transport
Breader	Processing	Other processing	Equipment used to coat meat/fish/poultry with a crumb coating
Briner	Processing	Other processing	Process to preserve food using a concentrated salt solution
Browner	Processing	Cooking	Equipment used to sear the outside surface of meats
Bulk storage	Storage	Other storage	Storage for a large amount of ingredient/product in a single container

(Continued)

Table 4.3 (Continued) CARVER+Shock Flow Process Possibilities			
Icon	Category	Subcategory	Description
Butcher	Processing	Meat processing	To cut up meat or poultry
Cans	Packaging	Packaging materials	Cylindrical metal container
Capper	Packaging		Applies caps to containers
Car	Storage	Other storage	Storage for a material waiting to be shipped
Caser	Packaging		Sorts and places product into cases
Centrifuge	Processing	Separation/ extraction	Machine that uses centrifugal force to separate substances with different densities
Check weigher	Control checks		A scale to check the weight of product
Chemicals	Materials	Processing materials	Cleaning chemicals
Chilled distribution	Transportation/ distribution		Refrigerated transport of product

Source: United States Food and Drug Administration, *CARVER+Shock Users' Manual* Version 1.0, 2007.

Each question has an associated score. Based on the answers given, the software calculates a score for each CARVER+Shock attribute and sums them to produce a total score for each node. Analogous to a face-to-face session, total scores range from 1 to 10 for each CARVER+Shock attribute and therefore from 7 to 70 for each node.

The interview questions seek to corroborate the flow process according to the variables under the CARVER acronym. Then, once the results are tabulated, a scoring system is linked to each of these variables. Table 4.4 displays the scoring criteria for accessibility.

Table 4.4 Carver+Shock Scoring Criteria	
Accessibility Criteria	Scale
Easily accessible (e.g., target is outside building and no perimeter fence). Limited physical or human barriers or observation. Attacker has relatively unlimited access to the target. Attack can be carried out using medium or large volumes of contaminant without undue concern of detection. Multiple sources of information concerning the facility and the target are easily available.	9–10
Accessible (e.g., target is inside building, but in unsecured part of facility). Human observation and physical barriers limited. Attacker has access to the target for an hour or less. Attack can be carried out with moderate to large volumes of contaminant but requires the use of stealth. Only limited specific information is available on the facility and the target.	7–8

(Continued)

Table 4.4 (Continued) Carver+Shock Scoring Criteria

Accessibility Criteria	Scale
Partially accessible (e.g., inside building, in a relatively unsecured, but busy, part of facility). Under constant possible human observation. Some physical barriers may be present. Contaminant must be disguised, and time limitations are significant. Only general, nonspecific information is available on the facility and the target.	5–6
Hardly accessible (e.g., inside building in a secured part of facility). Human observation and physical barriers with an established means of detection. Access generally restricted to operators or authorized persons. Contaminant must be disguised and time limitations are extreme. Limited general information available on the facility and the target.	3–4
Not accessible. Physical barriers, alarms, and human observation. Defined means of intervention in place. Attacker can access target for less than 5 minutes with all equipment carried in pockets. No useful publicly available information concerning the target.	1–2

This process relies on a comprehensive interview schema in order that calculations have reliability. In Figure 4.8, a sample interview page, published by the software, is provided.

CARVER+SHOCK DEFINITIONS

Criticality—A target is critical when the introduction of threat agents into food at this location would cause significant sickness, death, or economic impact.

Accessibility—A target is accessible when an attacker can reach the target, conduct the attack, and leave the target undetected.

Recognizability—A target's recognizability is the degree to which it can be identified by an attacker without confusion.

Vulnerability—Given a successful attack, vulnerability is the likelihood that the contaminant will achieve the attacker's purpose. It considers both processing steps and analytical steps at and downstream of the point of attack.

Effect—Effect is a measure of the percentage of system productivity damaged by an attack at a single facility. Thus, effect is inversely related to the total number of facilities producing the same product.

Recuperability—A target's recuperability is measured in the time it will take for the specific system to recover productivity.

Shock—Shock is the combined measure of the psychological and collateral national economic impacts of a successful attack on the target system. Shock is considered on a national level. The psychological impact will be increased if the target has historical, cultural, religious, or other symbolic significance. Mass casualties are not required to achieve widespread economic loss or psychological damage. Collateral economic damage includes such items as decreased national economic activity, increased unemployment in collateral industries, and so on. Psychological impact will be increased if victims are members of sensitive subpopulations, such as children or the elderly.

Internet Exercise: Visit the CARVER+Shock Primer webpage at <https://www.fda.gov/food/food-defense-programs/carver-shock-primer>.

Homeland Security

ABC Criticality category interview report

What is the serving size for the product? (If the product is used as an ingredient, how much of the product is used in each serving?)

What is the distribution unit (package size sold to the consumer)?

How many retail outlets typically receive units from one batch?

- ☐ 1
- ☐ 2–3
- ☐ 3–20
- ☐ >10

What percentage of each batch is sold...

—	Within one day of purchase?
—	Within first three days after purchase?
—	Within first two weeks after purchase?
—	Within first month after purchase?
—	During the first two months?

What percentage of the product is typically consumed ...

—	Within one day of purchase?
—	Within the first three days after purchase?
—	Within the first week after purchase?
—	Within two weeks after purchase?
—	Within first month after purchase?
—	Within first two months after purchase?

On average, how many individuals eat from the same distribution unit?

Does the company have a published support line for end consumers with concerns or questions?

- ☐ Yes
- ☐ No

Is there a formal company procedure for communicating information on a contamination incident to the public?

- ☐ Yes
- ☐ No

Does your company or facility have a mechanism in place to effectively implement a recall and withdraw product from the marketplace?

- ☐ Yes
- ☐ No

Does your company conduct mock product recalls?

- ☐ Yes
- ☐ No

How well can you trace your product to the distribution centers (D.C.s) and retail outlets?

- ☐ Cannot trace at all.
- ☐ Can identify independent D.C.s and entire distribution chains to major distributors that may have received units from one batch.
- ☐ Can trace specific pallets to independent D.C.s and entire distribution chains to major distributors such as Wal-Mart.
- ☐ Can identify all retail outlets that received units from a batch.
- ☐ Can trace specific pallets to each retail outlet that received it.

Is this product an uncoded product or uncoded raw ingredient?

- ☐ Yes
- ☐ No

Are you aware of large-scale counterfeiting or diversion for this product?

- ☐ Yes
- ☐ No

Figure 4.8 CARVER+Shock sample interview page.

4.3 Threats and Hazards

Threats come in many forms, and if anything is true about the last decade, it would be the evolution in the definition of threat. Some might argue that threats are those things emanating from military sources alone—in the form of armies or weaponry. Of even more compelling recent interest has been the emergence of the homegrown, domestic terrorist threat where our enemies reside among the populace, waiting to carry out the deed. This is part of what Secretary Janet Napolitano called the “New Threat Picture.”¹⁶ Over time and space, risks, threats, and vulnerabilities change or are altered. For example, a decade ago, the stress on cybersecurity would have seemed less important than it is today. Cyber clouds, cyber darkwebs and nets, hacking, and intrusions have now become a central feature of all threat analysis as the virtual world’s capacity for harm is just as significant as the real world.¹⁷

DHS and aligned agencies are addressing these virtual threats as keenly as the hurricane or flood, the lone wolf or the jihadi attack. A program called FedRamp.gov was erected in 2017 to coordinate our nation’s response to virtual threats. See Figure 4.9.¹⁸

Others might claim that a threat is driven by natural disasters or events that are unpredictable, such as a typhoon or hurricane. And still another conception deals with the threats of nuclear, chemical, and biological incidents. Threats and hazards are often distinguished by their motive and purpose. Hazards are generally construed as acts of nature; unintentional events without political motive or purpose. Threats, on the other hand, are usually bound to some improper aim or end, such as the political destruction of a government or the radical altering of leadership. Hurricanes and floods are events lacking any animus and, as such, are relegated to the hazard category.

What can be agreed on is that the United States daily remains subject to a host of threats and hazards from every imaginable direction. Professor Daniel Dunai, of Hungary’s National Defence University, graphically charts the onslaught in Figure 4.10.¹⁹

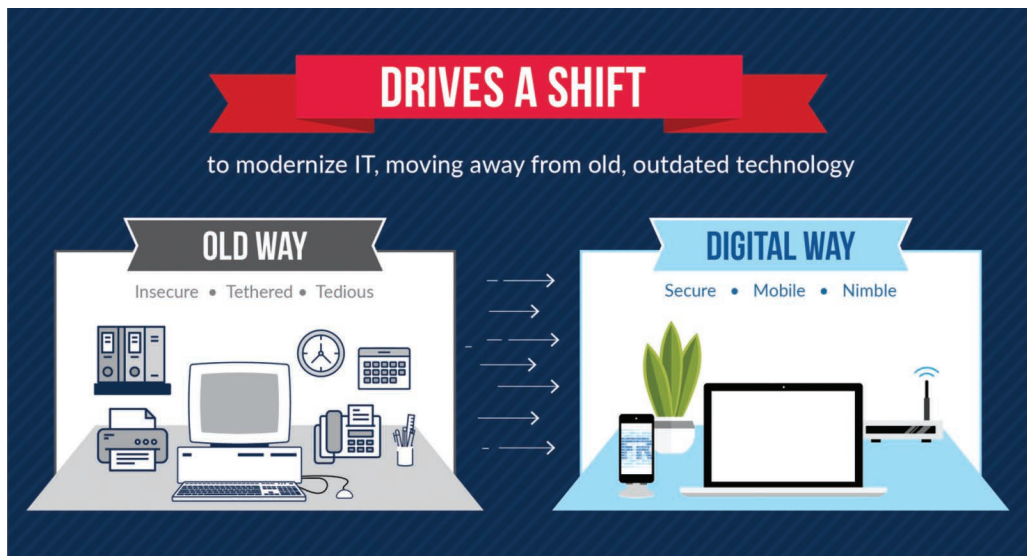


Figure 4.9 FedRamp encourages the modernization, thereby improving the security, of systems.

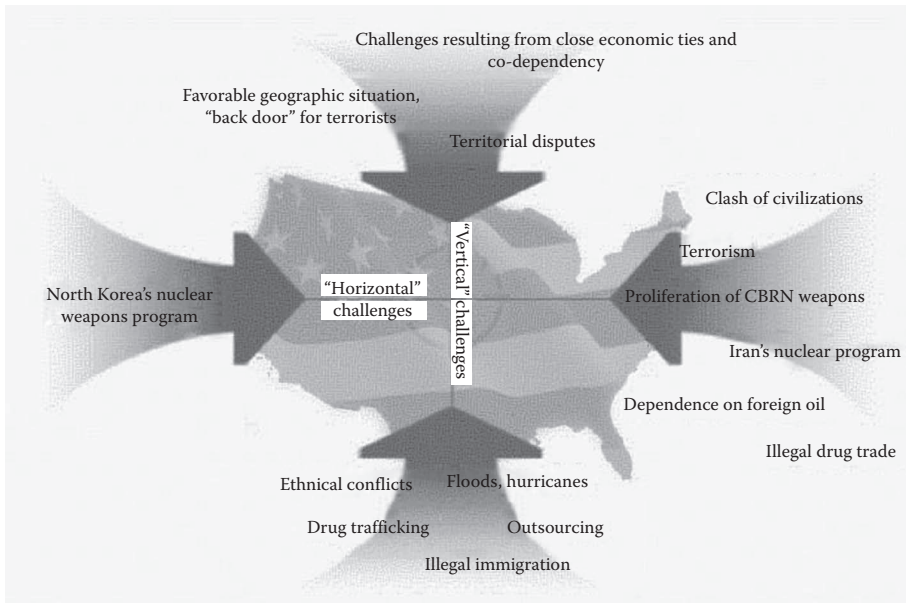


Figure 4.10 A convenient scheme for categorizing different threats and challenges.

4.3.1 Concept of Threat and Hazard

Natural hazards fall into these categories:

- Hurricanes
- Tornadoes
- Floods
- Winter storms
- Heat-related emergencies
- Droughts
- Wildfires
- Thunderstorms
- Geologic events

Government agencies and policy makers frequently underestimate the full impact of these natural disasters, at least as to the homeland defense mindset. These events wreak extraordinary havoc. The death toll alone is a distressingly impressive count (see Figure 4.11).²⁰

More than seven billion people worldwide have been negatively impacted by natural disasters in the last century—a statistic that lays out a permanent obligation for homeland personnel (see Figure 4.12).²¹

Threats fall into these typologies:

- Crimes
- Terrorism
- Unintentional events
- Blackouts

4.3 Threats and Hazards

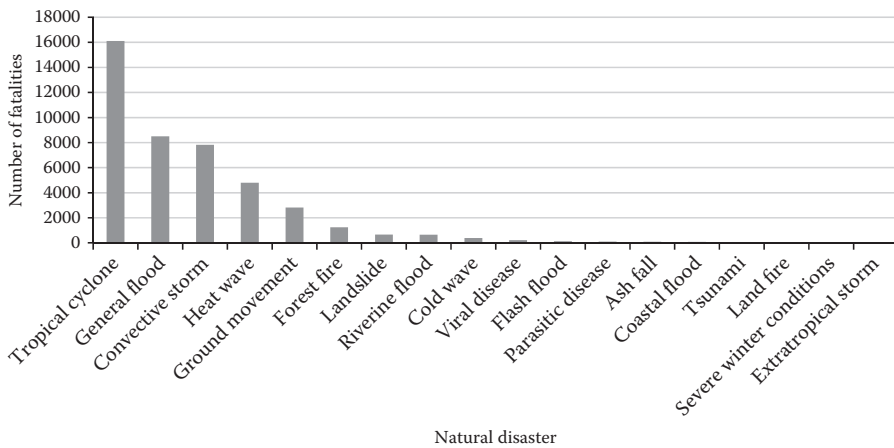


Figure 4.11 Fatalities from natural disasters in the United States from 1900 to 2015.

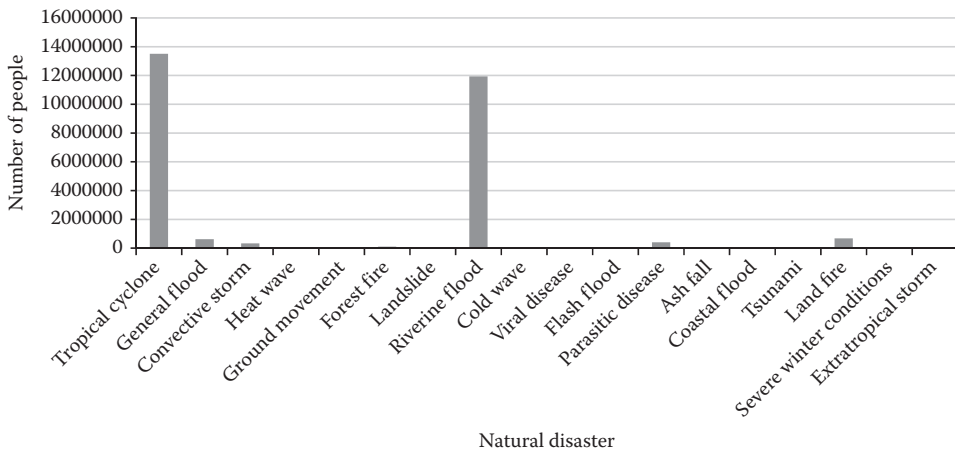


Figure 4.12 People affected by natural disasters in the United States from 1900 to 2015.

- Radiological events
- Hazmat incidents
- Fires

Threats arising from terrorism signify a malicious intent to intentionally threaten lives and property. These acts may range from a single person on a shooting rampage, to a cyber-attack that harms computer systems, to the organized use of WMD. WMD events could involve chemical, biological, explosive, or radioactive weapons. Acts of terrorism include threats of terrorism, assassinations, kidnappings, hijackings, bomb scares, and bombings. High-risk targets for acts of terrorism include military and civilian government facilities, international airports, large cities, and high-profile landmarks. Terrorists might also target large public gatherings, water and food supplies, utilities, and corporate centers. The 2015 attacks in France manifest this tendency to choose targets for maximum effect. In Paris, the choice of a soccer stadium, a concert hall, and public restaurants all achieve the underlying goal of the terrorist, which is to inflict

Homeland Security

maximum terror with maximum results. In Nice, it was one driver targeting crowds celebrating Bastille Day.

Internet Exercise: Visit CNN’s website and explore the videos on the Paris attacks: <http://www.cnn.com/2015/11/13/europe/paris-attacks-francois-hollande>.

Infrastructure of every variety needs constant vigilance in the matter of threat, from its original construction phase to its maintenance. Building design must anticipate threat even in terms of the materials used so that the structure might withstand natural disasters, blast, projectiles, and fire.²²

Identifying, anticipating, and defending against such a broad band of threats can only be described as daunting. For if homeland policy makers have learned anything over the last decade, it is that these concepts, like threat and disaster, have an evolutionary quality. The use of drones and unmanned equipment to deliver the punch of terror—even the various versions of WMD, should never be discounted. See Figure 4.13.²³

Other remote-controlled activities make risk prediction even more difficult. To illustrate, think how “autonomous” control of vehicles, controlled by outside influences rather than the owner or operator of the vehicle itself, can be a pathway to potential terror risk. A host of cases involving the hacking and intrusion into vehicle software programs, against the will and even knowledge of the owner, should generate great concern among homeland professionals.²⁴

In short, both the ideas and the means of execution change whether we admit it or not. Those entrusted must stay “in the box” as well as be capable of jumping “out of the box.” In other words, history tells us much about these events, although these same events may not evolve in just the way predicted. Alain Bauer’s insights on this dilemma are most helpful, for he urges the policy maker to find the commonality in all forms of terror. He argues that no matter what the group, what the religious sect, what the purpose or aim, all terrorists

- Have common harmonies
- Frequent common lands and territories
- Have a common (submerged) economy
- Offer real opportunities for symbiosis²⁵

Just as importantly, any analysis of a threat or a hazard will depend on its placement or target. Techniques regarding any threat and hazard tie to the locus of that activity. For example, airports



Figure 4.13 A small unmanned Clearpath Husky robot, which was used by ARL researchers to develop a new technique to quickly teach robots novel traversal behaviors with minimal human oversight (U.S. Army).

4.3 Threats and Hazards

have long been a favored location for jihadis looking to making great impacts or splashes. Airplane destruction—exploding out of the sky or using as projectiles into buildings—seem well ensconced in their tactics. But today, the terror threat and its prevention have shifted to the terminals, and even to the perimeter of the terminals with increasing cases of violence before ever encountering the TSA lines for screening. Using every intelligence method, be on the lookout for the following behaviors:

- Persons carrying bulky, excessively heavy, or oddly shaped baggage
- Individuals wearing clothing that does not meet the current environment, such as bulky outer garments, meant to conceal weapons or explosive materials
- Potential “swatting” threats that are intended to disturb transportation, or provoke a response
- Vehicles poorly parked, or displaying inappropriate/lacking identification tags
- The loss or theft of badges, ID cards, and access cards associated with the transit agency
- Unusual odors and/or hazardous or potentially hazardous materials, such as chemical, biological, or explosive materials, left at or near the office or facility
- Unusual questions about a facility or a transit asset’s purpose, operations, shifts, and/or security procedures on that transportation asset
- Individuals unable to display proper identification, or identification appears to be altered or fraudulent, including delivery personnel or contractors
- Individual(s) that inquire about transit schedules, operations, and procedures but fail to provide identification when asked.²⁶

What is abundantly clear is that the intelligence, emergency, and law enforcement communities must constantly anticipate how terror, threat, and vulnerability evolve and adapt to time and circumstance. What is favored today often is replaced by actions one could never conceive of.²⁷

Agencies and communities can chart potential threats by using the checklist in Table 4.5.

Of course, hazards can arise through human negligence and carelessness, which gives rise to a man-made catastrophe.

Table 4.5 Local Threats and Hazards

Type of Hazard	Likelihood of Occurrence	Potentially Devastating Impact on People	Potentially Devastating Impact on Structures
Natural Hazards			
Floods			
Winter storms			
Tornadoes			
Thunderstorm			
Hurricanes			
Extreme heat/cold			
Viral epidemics			

(Continued)

Table 4.5 (Continued) Local Threats and Hazards

Type of Hazard	Likelihood of Occurrence	Potentially Devastating Impact on People	Potentially Devastating Impact on Structures
Human-Induced Hazards			
Hazardous materials incidents			
Transportation accidents			
Infrastructure disruptions			
Workplace violence			
Civil disorder/disobedience			
Terrorist Hazards			
Conventional weapons			
Incendiary devices			
Biological and chemical agents			
Radiological			
Cyber-terrorism			
Weapons of mass destruction			

Source: Hazard Analysis and Vulnerability Study, done under contract to DC Emergency Management Agency, May 2002.

4.3.2 Weapons of Mass Destruction

No ambition is more glorifying for the terrorist than the successful delivery of a WMD. The terror associated with WMD is well founded and not to be addressed cavalierly.²⁸ The stuff of WMD can only be described as frightful and has the capacity to inflict global injury. There are four generally accepted categories of WMD, covered in the following subsections.

4.3.2.1 Nuclear

Some terrorist organizations, such as al Qaeda, openly declare their desire to acquire and use nuclear weapons. Even the complexities of devising a nuclear delivery mechanism are amply documented. Other nation states, like Iran and North Korea, continue to engage in nuclear weaponry production either openly or under the ruse of energy needs. North Korea's increasing testing of ICBM's and other long-range missile systems continue to worry the world at large. China and its growing arsenal remain a continuous threat to global security especially given its recent aggressive postures in the South China Sea and other disputed territories.²⁹

The array of intercontinental ballistic missiles continues to pose a day-to-day threat to most of civilization (see Figure 4.14).³⁰ The schematic in Figure 4.15³¹ gives some sense how extensive the damage can be from a nuclear strike.

The complete production of a nuclear weapon largely depends on the terrorist group's access to nuclear material and a high level of scientific expertise as well as the cooperation of rogue governmental regimes and terrorist leadership. Black-market materials can be utilized, though the crudeness of the enterprise is dangerous in and of itself (Figure 4.16).

Medium & Intermediate-Range Ballistic Missiles

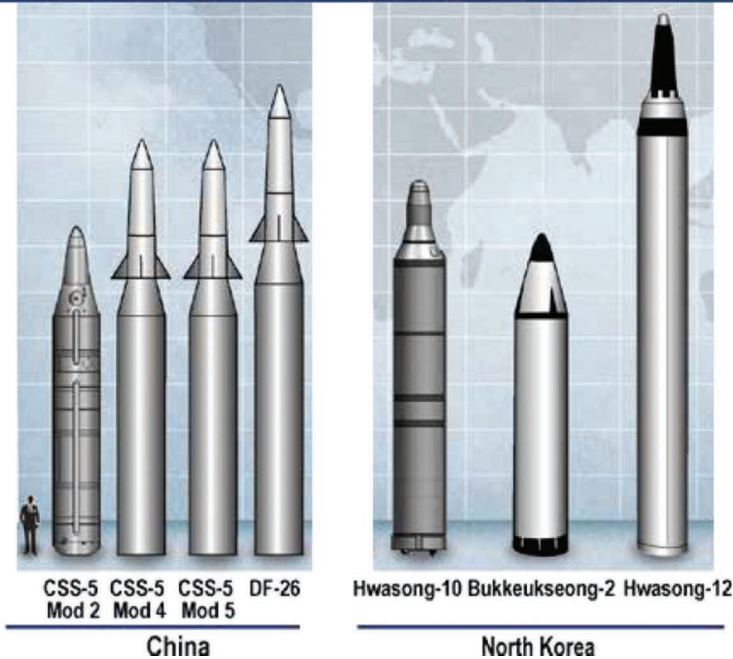


Figure 4.14 China and North Korea's medium- and intermediate-range ballistic missiles.

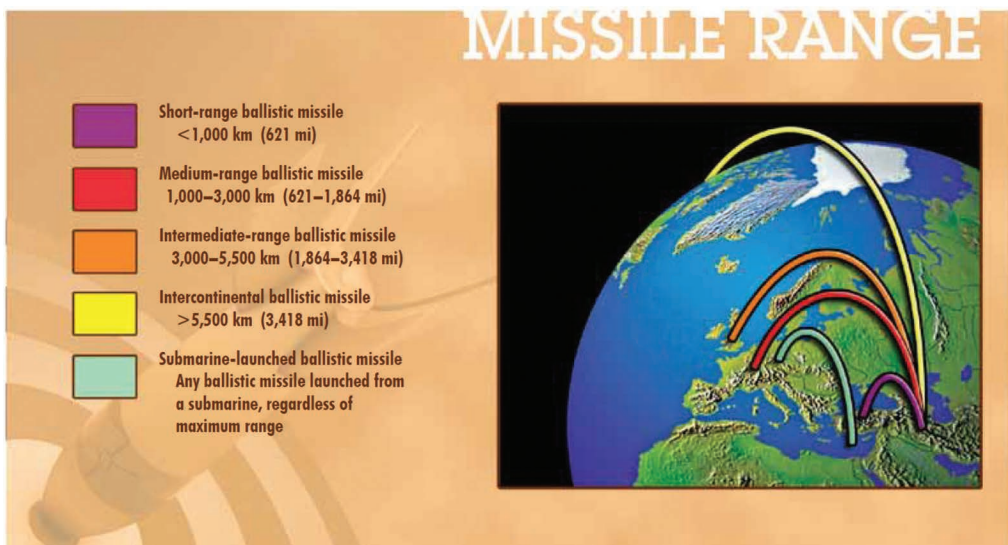


Figure 4.15 Visual schematic of the range of the various ranges of ballistic missiles.

DHS, by and through its Office of Domestic Nuclear Detection, is entrusted with the detection and prevention of nuclear terrorist threats. The basic objectives of the office are

- To develop the global nuclear detection and reporting architecture
- To develop, acquire, and support the domestic nuclear detection and reporting system



Figure 4.16 Nuclear power plant.

- To fully characterize detector system performance before deployment
- To establish situational awareness through information sharing and analysis
- To establish operation protocols to ensure detection leads to effective response
- To conduct a transformational research and development program
- To establish the National Technical Nuclear Forensics Center to provide planning, integration, and improvements to the U.S. government (USG) nuclear forensics capabilities.

The demands and complexities of nuclear threat call for constant and continuous assessment. Aside from perimeter concerns and access issues, the typical nuclear power facility not only utilizes physical materials capable of mass destruction but also must find ways to store and treat the by-products of nuclear power and production. Hence, DHS has recently tried to regularize practices in the nuclear industry regarding data storage and collection, physical security plans, and disposal.³² The organization of the Domestic Nuclear Detection Office is illustrated in Figure 4.17.

Physical security at nuclear power plants is provided by well-armed and well-trained security personnel who remain ready to respond to an attack 24 hours a day, 7 days a week. The sites are protected by sensitive intrusion detection equipment, fences, and barriers and are monitored by cameras and security patrols (Figure 4.18).

DHS has realized that the department cannot function in an isolated fashion when it comes to nuclear threat and that interagency cooperation is central to its mission. “Federal, state, local and private sector partners regularly and actively assess the risk environment in the Nuclear Sector in light of changes or potential changes to threats, vulnerabilities and consequences.”³³ In 2002, the Nuclear Regulatory Commission (NRC) announced the creation of the Office of Nuclear Security and Incident Response (NSIR) to improve NRC effectiveness in ensuring the protection of public health and safety from security threats at licensed facilities. On January 20, 2004, the commission announced the creation of the Emergency Preparedness Project Office (EPPO) to improve NRC’s effectiveness. On June 13, 2004, EPPO was integrated within NSIR, creating the Emergency Preparedness Directorate (EPD) and aligned the NRC’s preparedness, security, and incident response missions.

Nuclear terrorism can also be carried out at nuclear facilities. Each nuclear facility has high-level security responsibilities and must take seriously its charge to thwart any attempts on the facility. Nuclear facilities are required to have layers of security systems in place to prevent intrusion, contamination, the release of materials, or the loss or theft of radioactive and plutonium materials. In the most general terms, a security program for nuclear facilities minimally includes

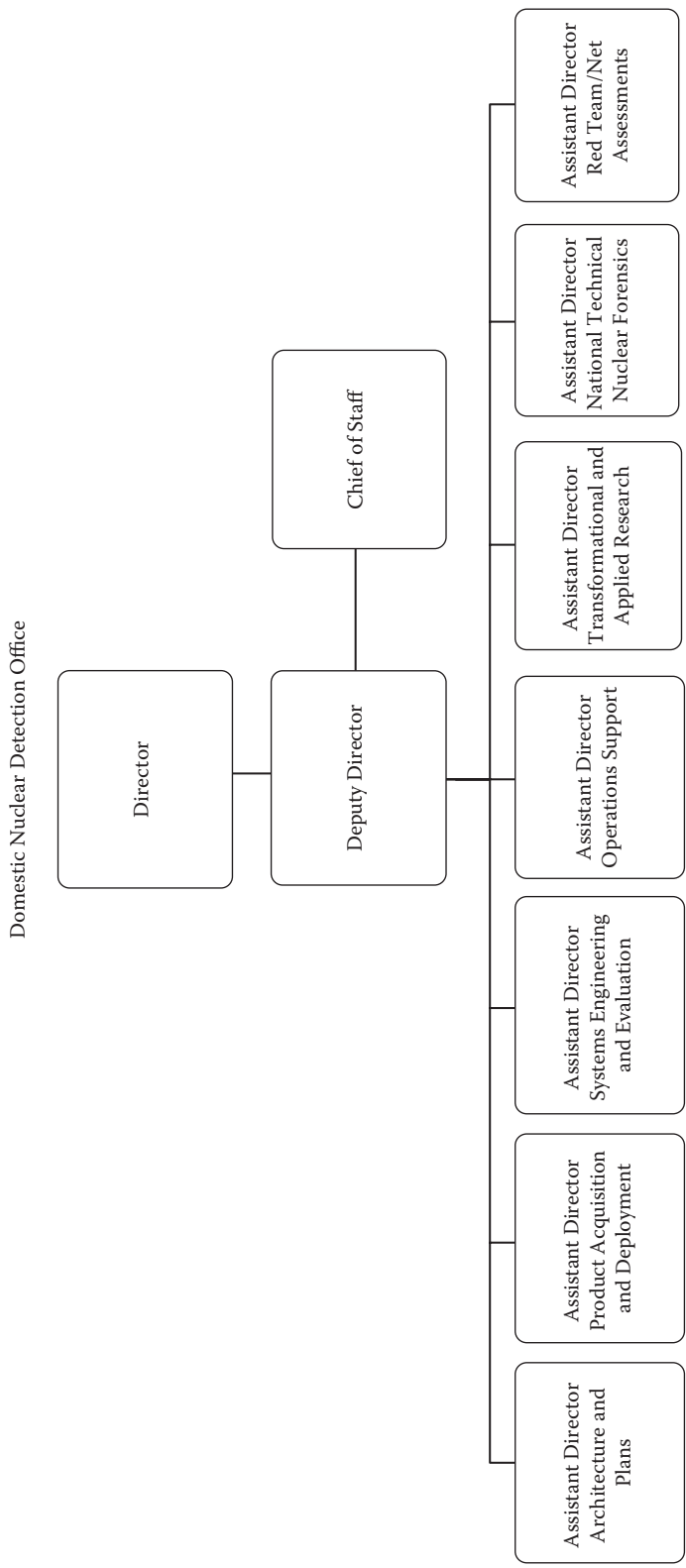


Figure 4.17 Organization chart of the office of Domestic Nuclear Detection Office.



Figure 4.18 Protection officer at a nuclear facility.

- A well-trained security force
- Robust physical barriers
- Intrusion detection systems
- Surveillance systems
- Plant access controls

In addition, nuclear facilities are required to conduct threat assessments regularly and are subject to regular and continuous security visitations by the NRC.

Internet Exercise: Visit the NRC web location for the results of security visits and requirements at plants throughout the United States at <http://www.nrc.gov/reading-rm/doc-collections/insp-manual/manual-chapter/mc0320.pdf>.

Training is rigorous and continuous. So concerned are the operators of nuclear reactors that extensive training, labeled *force on force* (FOF) training, anticipates an assault on the facility itself. Two sets of security officers—the first for maintenance of the actual facility and the other being the attack force—will engage one another in mock battle. The FOF exercise is highly realistic and essential to a preventive security program (see Figure 4.19).

The NRC requires nuclear power plant operators to defend the plant against attackers seeking to cause damage to the reactor core or spent fuel to prevent the release of radiation. Post assessment highlights any deficiencies in training and security protocol and is an important part of the day-to-day security plan at the facility.

As in all aspects of nuclear security, there must be clear lines of authority and agency cooperation at every level of government. In the event of a nuclear breach, the line between the NRC and DHS is precisely drawn, as shown in Figure 4.20.³⁴

Finally, in terms of response and advance mitigation, FEMA is entrusted with dealing with the effects and aftereffects of a nuclear blast. The extent of that participation will depend on a host of variables, including the size of the nuclear device, its detonation height, the nature of

NRC's FOF security exercises realistically test security forces' capability and security programs at nuclear power plants.



The NRC requires nuclear power plant operators to defend the plant against attackers seeking to cause damage to the reactor core or spent fuel, resulting in a release of radiation. During FOF exercises, a number of commando-style attacks are carried out against a plant's security forces, looking for deficiencies in the plant operator's defensive strategy. Any significant problems are promptly identified, reviewed, and fixed. Each nuclear power plant site will have at least one FOF exercise every three years. The NRC and plant operator ensure the safety of plant employees and the security of the plant during FOF exercises.

Figure 4.19 NRC Force on force training.

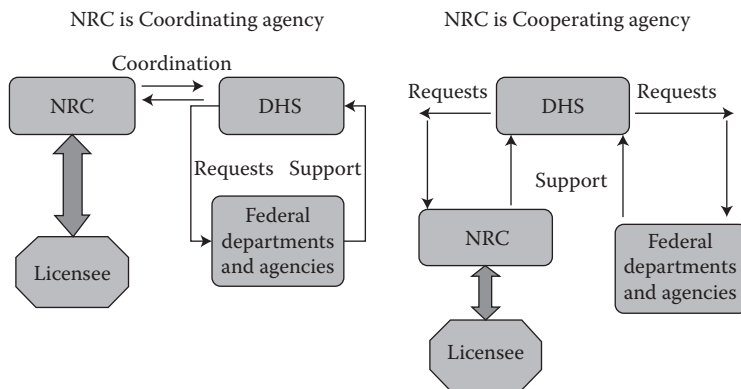


Figure 4.20 NRC interface with Department of Homeland Security.

the ground surface, and existing meteorological conditions. FEMA will not only encounter the damage resulting from blast and explosion but also the long-term effects of fallout.

Practitioners are now lucky enough to be able to conduct measurements for present and future harm regarding nuclear and radiological threats and consequences by modeling and software programs. The Radiological Assessment System for Consequence Analysis (RASCAL) is considered the industry's best example of this sort of measuring tool.

Internet Exercise: To gain an overview of how RASCAL works, visit <https://www.nrc.gov/docs/ML1008/ML100810144.pdf>.

4.3.2.2 Radiological

Some terrorists seek to acquire radioactive materials for use in a radiological dispersal device (RDD) or “dirty bomb.” In conjunction with the NRC, the Domestic Nuclear Detection Office is always on the hunt for individuals or groups intent on delivering nuclear WMD (Figure 4.21).

The most referenced threat in this sector is the use of a dirty bomb. The dirty bomb combines a conventional explosive, such as dynamite, with radioactive material. Upon detonation, aside from the immediate injuries inflicted, there will be severe collateral damage from the nuclear material itself.

The extent of local contamination will depend on several factors, including the size of the explosive, the amount and type of radioactive material used, the means of dispersal, and the weather conditions. The effects of radiation exposure are determined by

- Amount of radiation absorbed by the body
- Type of radiation (gamma, beta, or alpha)
- Distance from the radiation to an individual
- Means of exposure—external or internal (absorbed by the skin, inhaled, or ingested)
- Length of time exposed

See the graphic from the NRC in Figure 4.22 representing the various modes of exposure.

Most radioactive materials lack sufficient strength to present a significant public health risk once dispersed, and the materials posing the greatest hazard would likely infect the terrorists themselves.³⁵ The secondary and cultural effects of a dirty bomb would be quite acute since fear and panic would naturally be expected. The availability of radiological source material is more extensive than most know since this product is used widely in industrial, medical, and research applications; cancer therapy; food and blood irradiation techniques; and radiography.



Figure 4.21 Nuclear specialist at Nellis Air Force Base.

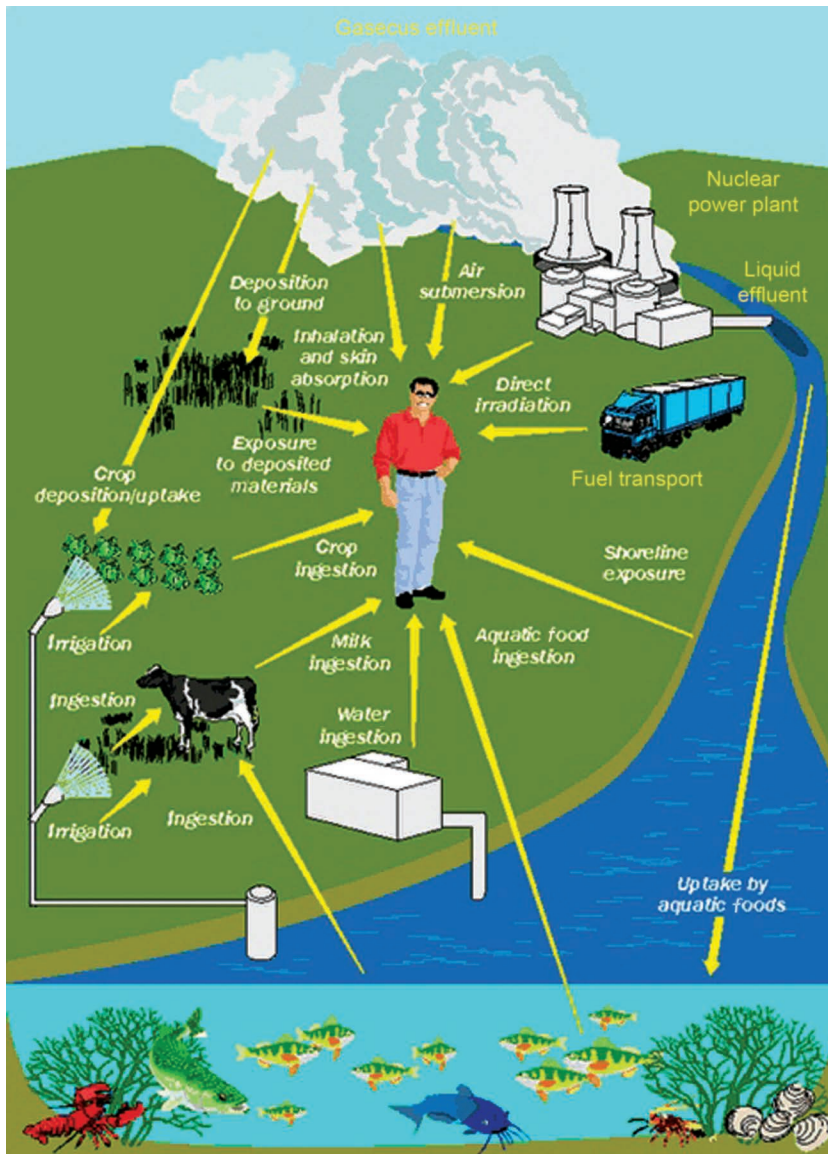


Figure 4.22 Radiation released in the environment will result in the exposure of general members of the public. The diagram shows some of the pathways that may lead to exposure.

Internet Exercise: To learn about survival steps in the event of a nuclear attack by a dirty bomb or other method, read the instructions issued by the Centers for Disease Control and Prevention (CDC) at <http://emergency.cdc.gov/radiation/dirtybombs.asp>.

Law enforcement takes the dirty bomb seriously, and agencies throughout the country regularly engage in tabletop or field exercises anticipating the dynamics of the event. In May 2003, DHS hosted a large, multiagency, and international exercise dealing with a dirty bomb in Seattle and a covert biological attack in Chicago. In all, 25 federal agencies, as well as the American Red Cross, were involved in the 5-day exercise, as well as partner agencies from the Canadian government. Overall, DHS continues its emphasis on exercises to give realism to its constituencies. In 2011, DHS announced a more formal “National Exercise Program,” which lays out a strategic



Figure 4.23 KINGSTON, NY—Soldiers from the 222nd Chemical Company in full hazardous material gear assist civilian participants during the decontamination phase of a joint force first-responders exercise in reaction to a radioactive attack. New York National Army and Airmen Guardsmen collaborate with local authorities to help train for the response to a radioactive terrorist attack, November 6, 2011. (Courtesy of Spc. Brian Godette, New York Army National Guard, 138th PAD.)

vision of how tabletop and other realistic programs can be used to prepare and mitigate security threats.³⁶

Aside from these broader exercises, DHS stressed particularized training to ensure the best possible response. The trend continues with regularly scheduled dirty bomb and disaster drills at federal, state, and local levels (Figure 4.23).

Internet Exercise: For an NRC fact sheet on dirty bombs, see <http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-dirty-bombs.html>.

4.3.2.3 Biological

Bioterrorism, another deadly threat and one discussed widely throughout this chapter, is the deliberate dispersal of pathogens through food, air, water, or living organisms in order to cause disease and other harm to the public. Biological agents can kill on a massive scale and have the potential to move quickly through large populations, leaving high rates of mortality.³⁷ Biological agents are, for the most part, tasteless, odorless, and invisible. The havoc occurs quickly and without much warning. Biological agents can be introduced by air, water, or in the food supply. FEMA categorizes agents by application, duration, extent of effects, and mitigation, as shown in Figure 4.24.

DHS has played an increasing role in this sort of detection. Through its Science and Technology Directorate, a series of programs that identify and detect biological agents have been implemented. Of recent interest is BioWatch—a program that measures air samples in 30 urban areas across the United States. Using BioWatch sensors, the technology monitors specific locations as well as events of national significance such as the Olympics or the Superbowl.³⁸ Figure 4.25 illustrates the latest generation in BioWatch technology, though there have been technical difficulties with version 3.³⁹

When compared with nuclear technology, this is a much easier scientific row to hoe, and anyone with some level of biological training and access to common laboratory equipment can develop terror tools that emerge from biological products. Biological agents, as the anthrax cases of the last decade demonstrate, foment high rates of fear in the general public (Figure 4.26).

The CDC assumes the preeminent position when it comes to the identification and mitigation of, the response to, and the recovery from a biological attack (see Figure 4.27).

Agent Type	Disease/Condition Caused by Agent	Description of Agent	Transmissible Person to Person	Infectivity/Lethality	Incubation Period	Duration of Illness	Persistence/ Stability	Vaccination/ Tonicity	Rate of Action	Symptoms	Treatment	Possible Means of Delivery
Bacterial	Botulism	Rod-shaped, gram-negative, aerobic, spore-forming (1-10 µm x 3-5 µm), highly resistant to heat and chemicals.	No	Moderate	1-7 days	3-5 days	Stable	Yes	Symptoms in 2-3 days. 24-36 hours after onset of symptoms.	Fever, malaise, fatigue, cough and mild chest discomfort, followed by severe respiratory distress, weakness, dysphagia, mydriasis, ataxia, and cyanosis.	Usually not effective after symptoms are present. High dose antibiotic treatment with penicillin, cephradine, or daptomycin should be undertaken. Supportive therapy may be necessary.	Animal
	Brucella	All non-motile, non-spore-forming, gram-negative, aerobic bacteria.	No	High/Low	Days to months	Weeks	Unstable in acid, stable in neutral and alkaline media.	Yes	Highly variable, usually 6-40 days.	Cough, sweat, dyspnea, fatigue, myalgia, arthralgia, and anorexia. Cough may occur after several weeks and is usually dry. Arthralgia, myalgia, and anorexia are usually accompanied by low-grade fever.	Recommended treatment is doxycycline (200 mg/day) plus rifampin (600 mg/day) for 6 weeks.	Animal. Expected to be delivered via aerosol.
	Cholera	Short, curved, motile, gram-negative, non-spore-forming, highly resistant to heat and chemicals.	Neg.	Low/High	1-5 days	1 or 2 weeks	Unstable in acid, stable in neutral and alkaline media.	Yes	Sudden onset after 1-5 day incubation period.	Initial vomiting and abdominal distention with little or no fever or abdominal pain. Followed by profuse watery diarrhea. Dehydration, hypotension, and shock.	Therapy consists of fluid and electrolyte replacement. Antibiotics will shorten the duration of illness. Tetracycline, erythromycin, and ampicillin are most commonly used. Fluoroquinolones are most commonly used.	1. Salinogen 2. Aerosol
	Clostridia	Gram-negative bacilli, primarily motile, rod-shaped, and highly resistant to heat and chemicals.	Neg.	Medium/High	10-14 days	NA	Stable	No	Initial onset of symptoms is usually 10-14 days after exposure.	Fluoroquinolones, tetracycline, and ampicillin are most commonly used. Clostridia may be delivered via aerosol.	Aerosol	Animal
	Plague (pneumonic, bubonic, septicemic)	Rod-shaped, non-motile, non-spore-forming, gram-negative, aerobic, highly resistant to heat and chemicals.	High	High/Very High	2 to 6 days	1-2 days	Stable	Yes	Two to three days	High fever, chills, headache, myalgia, and weakness, progressing rapidly to dyspnea, stupor, and cyanosis. Death results from respiratory failure, circulatory collapse, and a septicemic shock.	Early administration of antibiotics is very effective. Supportive therapy for pneumonia and septicemic forms is required.	May be delivered via aerosol, contact, or point source.
	Shigella	Rod-shaped, gram-negative, non-motile, non-spore-forming, highly resistant to heat and chemicals.	Neg.	High/Low	1-7 days	NA	Unstable in acid, stable in neutral and alkaline media.	No	Symptoms usually within 2-3 days, however, latent period may be as long as 12 hours or as long as 7 days.	Fever, nausea, vomiting, abdominal cramps, watery diarrhea, and occasionally, traces of blood in the feces. Symptom range from mild to severe with some affected individuals not experiencing any symptoms.	The antibiotics commonly used for treatment are penicillin, tetracycline, erythromycin, and ampicillin. Penicillin is usually the drug of choice. Supportive therapy is also required.	Contaminated food or water
	Staphylococcus aureus	Small, spherical, non-spore-forming, gram-positive, coagulase-positive, highly resistant to heat and chemicals.	No	High/Low	1-10 days	2 or 3 weeks	Stable	Yes	Three to five days	Uncomplicated staphylococcal infections with local ulcer and regional lymphadenopathy. Fever, chills, malaise, and general weakness. Systemic infection may be severe.	Administration of antibiotics with early treatment is very effective. Streptomycin - 1 gm i.v. 12 h x 10-14 d. Gentamicin - 5-7 mg/kg/day i.v. 12 h x 10-14 d.	Aerosol
	Typhoid	Rod-shaped, motile, non-spore-forming, gram-negative, highly resistant to heat and chemicals.	Neg.	Medium/High	6-21 days	Several weeks	Stable	Yes	One to three days	Sustained fever, severe headache, malaise, anorexia, a relative leukopenia, splenomegaly, non-productive cough in the early stage of the illness, and constipation more commonly seen in children.	Chemotherapy with chloramphenicol or TMP-SMX. Culture derivatives and first generation cephalosporins and supportive therapy.	Salivogen of food and water supplies.
	Yersinia enterocolitica	Non-motile, non-spore-forming, gram-negative, highly resistant to heat and chemicals.	No	High/High	10-20 days	2 weeks	Stable	Yes	Onset may be sudden.	Chills, reticular headache, weakness, malaise and severe sweat.	Tetracycline or doxycycline are the treatment of choice and are given orally for 5 to 7 days.	May be delivered via aerosol, contact, or point source.
	Yersinia enterocolitica	Non-motile, non-spore-forming, gram-negative, highly resistant to heat and chemicals.	No	High/High	6-15 days	Weeks	Stable	No	Variable onset, often sudden, after about 2 weeks of fever.	Headache, chills, prostration, fever, and general pain. A muscular eruption appears on the trunk and limbs. Rash is usually not the face, palms, or soles.	Tetracycline or doxycycline orally in a loading dose of 2-3 g, followed by daily doses of 1-2 g in 4 divided doses oral or intravenous antibiotic therapy 2 days post 1 day.	May be delivered via aerosol, contact, or point source.
Viral	Encephalitis	Non-motile, non-spore-forming, highly resistant to heat and chemicals.	Neg.	High/High	5-15 days	1-3 weeks	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Flavivirus	Non-motile, non-spore-forming, highly resistant to heat and chemicals.	Low	High/Low	1-5 days	Days to weeks	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Flavivirus	Non-motile, non-spore-forming, highly resistant to heat and chemicals.	Moderate	High/High	7-8 days	5-10 days	Stable	No	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Flavivirus	Non-motile, non-spore-forming, highly resistant to heat and chemicals.	Moderate	High/High	3-6 days	1-2 weeks	Stable	No	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Flavivirus	Non-motile, non-spore-forming, highly resistant to heat and chemicals.	Neg.	High/High	1-5 days	1-2 weeks	Stable	No	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Flavivirus	Non-motile, non-spore-forming, highly resistant to heat and chemicals.	High	High/High	7-17 days	1-2 weeks	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Flavivirus	Non-motile, non-spore-forming, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Flavivirus	Non-motile, non-spore-forming, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Flavivirus	Non-motile, non-spore-forming, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Flavivirus	Non-motile, non-spore-forming, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
Toxin	Botulinum Toxin	Protein, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Botulinum Toxin	Protein, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Botulinum Toxin	Protein, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Botulinum Toxin	Protein, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Botulinum Toxin	Protein, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Botulinum Toxin	Protein, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Botulinum Toxin	Protein, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Botulinum Toxin	Protein, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Botulinum Toxin	Protein, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Botulinum Toxin	Protein, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.
	Botulinum Toxin	Protein, highly resistant to heat and chemicals.	No	High/High	Variable (1-10 days)	2-72 hours	Stable	Yes	Sudden	Inflammation of the meninges of the brain. Headache, fever, dizziness, and ataxia.	No specific treatment; supportive treatment is essential.	Aerosol spread possible.

Figure 4.24 Selected biological agent characteristics.

Homeland Security



Figure 4.25 BioWatch: Generation 3 monitoring station. DHS.

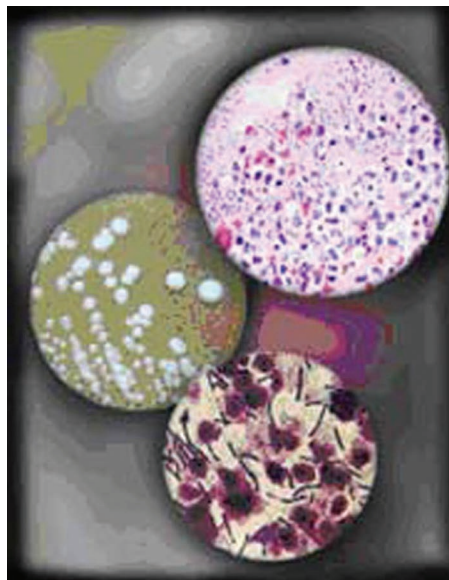


Figure 4.26 Biological agents under a high-powered microscope.

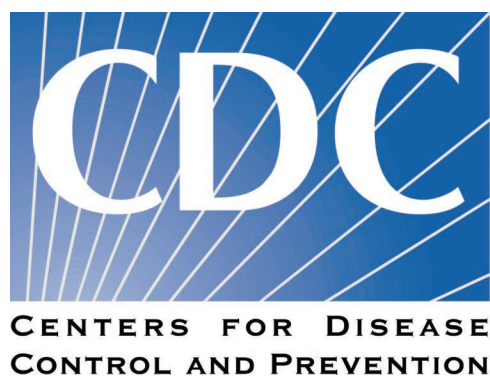


Figure 4.27 Centers for Disease Control and Prevention logo.

It classifies biological agents into three major categories:

Category A diseases/agents: The U.S. public health system and primary health-care providers must be prepared to address various biological agents, including pathogens that are rarely seen in the United States. High-priority agents include organisms that pose a risk to national security because they

- Can be easily disseminated or transmitted from person to person
- Result in high mortality rates and have the potential for major public health impact
- Might cause public panic and social disruption
- Require special action for public health preparedness

Category B diseases/agents: Second highest priority agents include those that

- Are moderately easy to disseminate
- Result in moderate morbidity rates and low mortality rates
- Require specific enhancements of the CDC's diagnostic capacity and enhanced disease surveillance

Category C diseases/agents: Third highest priority agents include emerging pathogens that could be engineered for mass dissemination in the future because of

- Availability
- Ease of production and dissemination
- Potential for high morbidity and mortality rates and major health issues

The CDC types of all known biological agents are listed into these three categories.⁴⁰ As of 2015,⁴¹ the list of biological agents was composed of

- Anthrax (*Bacillus anthracis*)
- Arenaviruses
- *Bacillus anthracis* (anthrax)
- Botulism (*Clostridium botulinum* toxin)
- Brucella species (*brucellosis*)
- *Brucellosis* (Brucella species)
- *Burkholderia mallei* (glanders)
- *Burkholderia pseudomallei* (melioidosis)
- *Chlamydia psittaci* (psittacosis)
- Cholera (*Vibrio cholerae*)
- *Clostridium botulinum* toxin (botulism)
- *Clostridium perfringens* (Epsilon toxin)
- *Coxiella burnetii* (Q fever)
- Ebola virus hemorrhagic fever
- *E. coli* O157:H7 (*Escherichia coli*)
- Emerging infectious diseases such as Nipah virus and hantavirus
- Epsilon toxin of *Clostridium perfringens*
- *Escherichia coli* O157:H7 (*E. coli*)

Homeland Security

- Food safety threats (e.g., salmonella species, *E. coli* O157:H7, shigella)
- *Francisella tularensis* (tularemia)
- Glanders (*Burkholderia mallei*)
- Lassa fever
- Marburg virus hemorrhagic fever
- Melioidosis (*Burkholderia pseudomallei*)
- Plague (*Yersinia pestis*)
- Psittacosis (*Chlamydia psittaci*)
- Q fever (*Coxiella burnetii*)
- Ricin toxin from *Ricinus communis* (castor beans)
- *Rickettsia prowazekii* (typhus fever)
- Salmonella species (salmonellosis)
- *Salmonella typhi* (typhoid fever)
- Salmonellosis (salmonella species)
- Shigella (shigellosis)
- Shigellosis (shigella)
- Smallpox (*Variola major*)
- Staphylococcal enterotoxin B
- Tularemia (*Francisella tularensis*)
- Typhoid fever (*Salmonella typhi*)
- Typhus fever (*Rickettsia prowazekii*)
- *Variola major* (smallpox)
- *Vibrio cholerae* (cholera)
- Viral encephalitis (alphaviruses [e.g., Venezuelan equine encephalitis, eastern equine encephalitis, western equine encephalitis])
- Viral hemorrhagic fevers (filoviruses [e.g., Ebola, Marburg] and arena-viruses [e.g., Lassa, Machupo])
- Water safety threats (e.g., *Vibrio cholerae*, *Cryptosporidium parvum*)

For the present, the bulk of attention has been on four to five biological agents with the potential for severe harm. A summary analysis of these follows.

4.3.2.3.1 Anthrax

Few words evoke the terror that anthrax does. Anthrax has a long history of infecting nations and individuals, and even today it does not respond readily to medical intervention. Anthrax is caused by *B. anthracis*, a disease-causing bacterium that forms spores. A spore is a cell that is dormant (asleep) but over time may arise from its slumber.

Anthrax can be broken down anatomically:

- Skin (cutaneous)
- Lungs (inhalation)
- Digestive (gastrointestinal)

4.3 Threats and Hazards

The diagnosis of anthrax will be evidenced by certain warning signs in the infected party and where the disease has found a home:

- *Cutaneous*: Initial symptoms are blisters that eventually turn black.
- *Gastrointestinal*: Symptoms are nausea, loss of appetite, bloody diarrhea, fever, and significant stomach pain.
- *Inhalation*: Cold or flu symptoms, including a sore throat, mild fever, and muscle aches. Later symptoms include cough, chest discomfort, shortness of breath, tiredness, and muscle aches.

The effects of anthrax on the human body are both painful and extreme (Figure 4.28).

Without care, death is the fate of the infected party. Remediation of anthrax will be dependent on its stage and the party's resistance to antibiotics. The sooner medical attention is sought, the better the cure.

Emergency providers include anthrax in their planning and preparedness model. In general, the emergency plan should include

- Response plans and procedures for anthrax
- Training and equipping emergency response teams
- Collaborative arrangements with health departments, veterinarians, and laboratories to watch for suspected cases of anthrax
- Sufficient laboratories for quick testing of suspected anthrax cases
- Sufficient medical supplies

The Coast Guard and the four branches of the U.S. military are so concerned that anthrax may be used in conflict against them that all military branches launched the Anthrax Vaccine Immunization Program (AVIP). See the general order implementing the AVIP program for all personnel in Figure 4.29.



Figure 4.28 Anthrax infection. (Courtesy of Anthrax Vaccine Immunization Program for Combined Services.)



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

OCT 12 2006

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL, DEPARTMENT OF DEFENSE
INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
DIRECTORS OF DEFENSE AGENCIES
COMMANDANT OF THE US COAST GUARD

SUBJECT: Anthrax Vaccine Immunization Program

Based on the continuing heightened threat to some U.S. personnel of attack with anthrax spores, the Department of Defense will resume a mandatory Anthrax Vaccine Immunization Program, consistent with Food and Drug Administration guidelines and the best practice of medicine, for designated military personnel, emergency-essential and comparable Department of Defense civilian employees, and certain contractor personnel performing essential services. Vaccination is mandatory for these personnel based on geographic area of assignment or special mission roles, except as provided under applicable medical and administrative exemption policies.

As it was under the Deputy Secretary of Defense Memorandum of June 28, 2004, "Expansion of Force Health Protection Anthrax and Smallpox Immunization Programs for DoD Personnel," the scope of the mandatory Anthrax Vaccine Immunization Program shall encompass personnel assigned to or deployed for 15 or more consecutive days in higher-threat areas and certain other personnel with special mission roles. Other personnel determined by the Assistant Secretary of Defense for Health Affairs, in consultation with the Chairman of the Joint Chiefs of Staff, to be at higher risk of exposure to anthrax may also be included in the program. Vaccinations shall begin, to the extent feasible, up to 60 days prior to deployment or arrival in higher-threat areas.

Consistent with the FDA-approved guidelines for use of anthrax vaccine, all personnel who begin the six-dose vaccine series (unless excluded for medical reasons) will be offered all six doses and the annual booster as long as they remain members of the armed forces or maintain a civilian employee or contractor status covered by the program. For those no longer deployed to a higher threat area or no longer assigned designated special mission roles, these later vaccine doses will be on a voluntary basis. Individuals whose vaccine series was interrupted are not required to restart the vaccine series, but will proceed in accordance with appropriate medical practice.



Figure 4.29 General Order from the Deputy Secretary of Defense implementing the Anthrax Vaccine Immunization Program (AVIP) for all personnel.

4.3.2.3.2 Plague

The term plague conjures up images of the Dark Ages, when disease ravaged the countryside, killing millions over short periods of time. Yet, plague is a very real phenomenon that those concerned about biological attacks should never forget. Just as in centuries past, plague is an infectious bacterium carried by rats, flies, and fleas. Plague is an infectious airborne disease that affects others who come into contact with its strain of bacteria. Plague is normally transmitted

from an infected rodent to humans by infected fleas. Bioterrorism-related outbreaks are likely to be transmitted through the dispersion of an aerosol. Person-to-person transmission of pneumonic plague is possible by a large dose of aerosol droplets. Indeed, many describe the COVID-19 virus as the full image of what a plague is. Certainly, the level of its death and overall harm were never projected as even possible a few months ago.

There are three kinds of plague:

- Pneumonic plague can spread from person to person through the air. Transmission can take place if someone breathes in aerosolized bacteria, which could happen in a bioterrorist attack.
- Bubonic plague is the most common form of plague. This occurs when an infected flea bites a person or when materials contaminated with *Y. pestis* enter through a break in a person's skin.
- Septicemic plague occurs when plague bacteria multiply in the blood. It can be a complication of pneumonic or bubonic plague, or it can occur by itself.

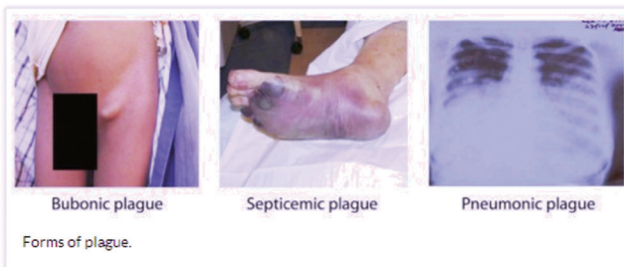
Several terrorist groups and some nations are experimenting with biological weapons programs. Plague could be used in an aerosol that would cause the pneumonic version. Once the disease is contracted, the bacteria can spread to others by close contact. Bubonic plague could be generated by releasing plague-infected fleas or animals. The *Y. pestis* bacterium occurs in nature and is also widely available in microbiology laboratories around the world. Thousands of scientists are working with plague organisms daily (see Figure 4.30).⁴²

[CDC > Plague Home](#)

Symptoms



Plague symptoms depend on how the patient was exposed to the plague bacteria. Plague can take different clinical forms, but the most common are bubonic, pneumonic, and septicemic.



Bubonic plague: Patients develop sudden onset of fever, headache, chills, and weakness and one or more swollen, tender and painful lymph nodes (called buboes). This form usually results from the bite of an infected flea. The bacteria multiply in the lymph node closest to where the bacteria entered the human body. If the patient is not treated with the appropriate antibiotics, the bacteria can spread to other parts of the body.

Septicemic plague: Patients develop fever, chills, extreme weakness, abdominal pain, shock, and possibly bleeding into the skin and other organs. Skin and other tissues may turn black and die, especially on fingers, toes, and the nose. Septicemic plague can occur as the first symptom of plague, or may develop from untreated bubonic plague. This form results from bites of infected fleas or from handling an infected animal.

Pneumonic plague: Patients develop fever, headache, weakness, and a rapidly developing pneumonia with shortness of breath, chest pain, cough, and sometimes bloody or watery mucous. Pneumonic plague may develop from inhaling infectious droplets or may develop from untreated bubonic or septicemic plague after the bacteria spread to the lungs. The pneumonia may cause respiratory failure and shock. Pneumonic plague is the most serious form of the disease and is the only form of plague that can be spread from person to person (by infectious droplets).

Plague is a serious illness. If you are experiencing symptoms like those listed here, seek immediate medical attention. Prompt treatment with the correct medications is critical to prevent complications or death.

Figure 4.30 CDC's web page on plague symptoms.

Homeland Security

If detected early enough, antibiotics can be effective. A vaccine has yet to be developed.

Internet Exercise: Visit the CDC Plague Information webpage by visiting <https://emergency.cdc.gov/agent/plague/> and clicking on the CDC Plague Home Page link.

4.3.2.3.3 *Smallpox*

Smallpox has been referred to as the king of bioterrorism due to its ease of transmission and simplicity of delivery. It was the scourge of many a nation until its almost complete eradication in the 1970s. Unfortunately, the world has seen a return of this virulent disease and, just as distressingly, has heard of its potential to be a weapon of mass destruction. Smallpox is a serious, contagious, and sometimes fatal infectious disease. Smallpox comes in two varieties: *V. major*, the most severe and most common form of smallpox; and *V. minor*, a less common presentation of smallpox with medical effects.

There is no specific treatment for smallpox, and the only prevention is vaccination. Generally, direct and fairly prolonged face-to-face contact is required to spread smallpox, usually by saliva, from one person to another. Smallpox can also be spread through direct contact with infected bodily fluids or contaminated objects (Figure 4.31).

Smallpox has the capacity to inflict horrid damage and is considered part of the arsenal for the terrorist. Containment and isolation are urgent requirements. Calming the public, the victims' families, and loved ones is another essential task. The CDC publishes protocols on how to handle the smallpox case—from the initial communications chain to isolation, vaccination, and subsequent media demands. Use the checklist in Table 4.6 to organize that sort of operation.⁴³

Internet Exercise: The United Nations (UN) has dedicated a good portion of its resources to the eradication of biological weapons. The UN library in Geneva is an excellent source center for data and literature on these efforts. Visit the library at <https://digitallibrary.un.org/?ln=en>.

4.3.2.4 Chemical

Chemical weapons represent another form of WMD for terrorists. Chemical weapons have seen usage in both accidental and intentional terms. For example, the release of chemical toxins in an industrial accident can wreak havoc on the public health. More maliciously, the intentional



Figure 4.31 The rash and body lesions that result from smallpox are intense and unrivaled in epidemiology. Less than a week after an infection, the results are plain enough.

Table 4.6 Team Leader's List of Actions and Decisions to Be Considered

Action or Decision	Lead Person— State or Local HD	Lead Person— CDC Team
Identify key decision-makers and infrastructure at State and local HD		
Identify with above officials the counterparts for CDC team members		
Identify and review existing state/local emergency or BT plans		
Identify state/local chains of command for action- and decisions and communications and agree on access points		
Negotiate roles of CDC team in collaboration with State/local officials		
Identify office space, transport, and facilities for team members		
Identify and clarify roles of press spokespersons		
Review smallpox response plan and priority task lists and establish plan for implementation		
Identify other state/local/federal agencies involve and their roles		
Identify serious issues (isolation policy, quality of medical care vs. isolation) for which immediate, high-level discussions and decisions are needed—note eight areas below • Immediate need to determine number and composition and identify personnel for state/local first response team and facilities such as vaccination clinics and isolation/hospitals, assure training, vaccination, transport, and other support needs • Surveillance/reporting—provider and public health alert system; laboratory alert system; active/passive rash illness reporting networks; ER alert; case response plan in place; source of exposure; data compiling support • Contact and contacts of contact identification, tracing, vaccination, surveillance for fever/rash, vaccine site, and severe adverse events; risk prioritization for contact tracing • Vaccination policy(s): who, where, when, and by whom; containment or containment and mass; fixed vaccination clinics, household/neighborhood vaccination, mobile teams; separate vaccination sites for contacts, response teams, and essential services (police, water, power, fireman, other security groups, child health services, etc; smallpox vaccine storage, distribution, and security • Decide on isolation policy(s): home, hospital, smallpox isolation facility; transport of cases; security, enforcement, and maintenance issues; level of medical care to be provided		

(Continued)

Table 4.6 (Continued) Team Leader's List of Actions and Decisions to Be Considered

Action or Decision	Lead Person— State or Local HD	Lead Person— CDC Team
• Status of State quarantine rules/laws and who and how would they be implemented • Training and educational plans: supplies of educational and training materials; facilities, trainers, schedules needed; various curricula; identifying personnel to be trained; web-based and other alternatives for training and education • Security arrangements for all team members; plans for controlling the population and enforcement of vaccination and isolation • Supplies on hand/needed such as: bifurcated needles, forms of many types. Spox disease identification cards, vaccine take cards, VIS (languages), and so on		
Delegate assignments reflecting above needs and begin implementation with written notes of persons responsible and deadlines		
Identify political officials needed (e.g., Governor and Mayor) to reach decision quickly		
Reach consensus and schedule daily (or more frequent) meetings with key officials		
Schedule phone briefings and meetings with team members daily		
Arrange conference calls with CDC “Smallpox central” in Atlanta		

infliction of chemical toxins by a terrorist manifests their mindset and a complete and utter disregard for human life. In World War I, soldiers on the trench fronts experienced the ferocity and terminal quality of various chemical gases. Chemical weapons can cause high levels of mortality. This conflict is often referred to as the chemist's war, and the range, depth, and breadth of usage shocks even today's hardened soldier. These agents could cause mass casualties, as demonstrated by the use of chemical weapons during World War I (see Table 4.7).

Today's terrorist threat is just as real and dangerous. As recently as 1995, the Tokyo subway was flooded with sarin gas, delivered via plastic bottles; it is miraculous that more injuries and deaths did not occur.

More recently, terrorists have concentrated on acquiring and employing chemical materials with dual uses, such as pesticides, poisons, and industrial chemicals. In the Syrian Civil War, chemical attacks—once a declared “red line” by the Obama administration—have been unfortunately far too common,⁴⁴ and all use of chemical weaponry has been largely agreed to by the community of nations.⁴⁵

Chemical threats come in a variety of forms and delivery systems. These agents are far more common and much easier to develop and distribute than their biological and nuclear counterparts. Many household products, farm fertilizers, and other agricultural and industrial products contain the elements necessary to shape chemical terror. Access to chemical materials is fairly free. College and university labs, commercial labs, and medical facilities often have direct access to materials that can be used for nefarious purposes. Persons claiming to be college officials or

Table 4.7 Types of Chemical Weapons Utilized in World War I

Name	First Use	Type
Chlorine	1915	Irritant/lung
Phosgene	1915	Irritant/skin and mucous membranes, corrosive, toxic
Chloromethyl chloroformate	1915	Irritant/eyes, skin, lungs
Trichloromethyl chloroformate	1916	Severe irritant, causes burns
Chloropicrin	1916	Irritant, lachrymatory, toxic
Stannic chloride	1916	Severe irritant causes burns
α -Chlorotoluene (benzyl chloride)	1917	Irritant, lachrymatory
Bis(chloromethyl) ether (dichloromethyl ether)	1918	Irritant can blur vision
Diphenylchloroarsine (diphenyl chlorasine)	1917	Irritant/sternutatory
Ethylchloroarsine	1918	Vesicant
N-Ethylcarbazole	1918	Irritant
Benzyl bromide	1915	Lachrymatory
Ethyl iodoacetate	1916	Lachrymatory
Bromoacetone	1916	Lachrymatory, irritant
Bromomethyl ethyl ketone	1916	Irritant/skin, eyes
Acrolein	1916	Lachrymatory, toxic
Hydrocyanic acid	1916	Paralyzing
Hydrogen sulfide	1916	Irritant, toxic
Mustard gas	1917	Vesicant (blister)

students entrusted with lab responsibilities have been apprehended using fraudulent titles and addresses at universities to gain access to restricted chemical materials.⁴⁶

The general typology of chemical agents includes

- *Biotoxins*—Poisons that come from plants or animals
- *Blister agents/vesicants*—Chemicals that severely blister the eyes, respiratory tract, and skin on contact
- *Blood agents*—Poisons that affect the body by being absorbed into the blood
- *Caustics (acids)*—Chemicals that burn or corrode people's skin, eyes, and mucus membranes
- *Choking/lung/pulmonary agents*—Chemicals that cause severe irritation or swelling of the respiratory tract
- *Incapacitating agents*—Agents that can affect consciousness
- *Long-acting anticoagulants*—Poisons that prevent blood from clotting properly
- *Metals*—Agents that consist of metallic poisons

Homeland Security

- *Nerve agents*—Highly poisonous chemicals that work by preventing the nervous system from working properly
- *Organic solvents*—Agents that damage the tissues of living things by dissolving fats and oils
- *Riot control agents/tear gas*—Highly irritating agents normally used by law enforcement for crowd control
- *Toxic alcohols*—Poisonous alcohols that can damage the heart, kidneys, and nervous system
- *Vomiting agents*—Chemicals that cause nausea and vomiting

Internet Exercise: Find out more about chemical threats by visiting the National Institute of Occupational Safety and Health (NIOSH) pocket guide on chemical threats at <http://www.cdc.gov/niosh/npg>.

The sheer volume of chemical agents makes full coverage impossible. Those agents most likely to be encountered in the world of homeland security will be part of this overview (see Figure 4.32).

4.3.2.4.1 Ricin

Ricin is a poison found naturally in castor beans. Ricin can be made from the waste material left over from processing castor beans (Figure 4.33).

Ricin may be produced in various forms, including powder, mist, or pellet. It can also be dissolved in water or weak acid. Castor beans are processed throughout the world to make castor oil, and its by-product, the “mash,” provides the source material for the dangerous chemical.

The production is not a natural by-product but an intentional manufacture, which indicates malevolence on the part of the maker of the ricin. Ricin can be delivered in various ways, including

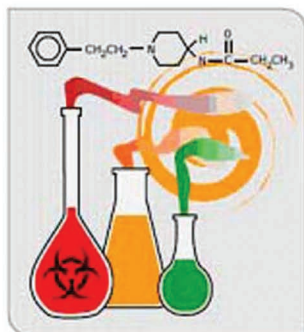
- *Indoor air:* Ricin can be released into indoor air as fine particles (aerosol).
- *Water:* Ricin can be used to contaminate water.
- *Food:* Ricin can be used to contaminate food.
- *Outdoor air:* Ricin can be released into outdoor air as fine particles.
- *Agricultural:* If ricin is released into the air as fine particles, it can damage and contaminate agricultural products.

Ricin can be absorbed into the body through ingestion, inhalation, or eye contact. Ricin can be absorbed through open skin or wounds but most likely not through intact skin, unless aided by a solvent. Ricin causes acute respiratory problems, impacts central organs in the human body, and can negatively affect eyes and ears. It can cause death in less than 24 hours (Figure 4.34).

Clues that indicate the presence or release of ricin include but are not limited to

- An unusual increase in the number of patients seeking care for potential chemical release–related illness
- Unexplained deaths among young or healthy persons
- Emission of unexplained odors by patients
- Clusters of illness in persons who have common characteristics, such as drinking water from the same source
- Rapid onset of symptoms after an exposure to a potentially contaminated medium
- Unexplained death of plants, fish, or animals (domestic or wild)
- A syndrome suggesting a disease associated commonly with a known chemical exposure (e.g., neurologic signs or pinpoint pupils in eyes of patients with a gastro-enteritis-like syndrome or acidosis in patients with altered mental status)⁴⁷

BE INFORMED CHEMICAL THREAT



1. A chemical attack is the deliberate release of a toxic gas, liquid or solid that can poison people and the environment.



2. Watch for signs such as many people suffering from watery eyes, twitching, choking, having trouble breathing or losing coordination.



3. Many sick or dead birds, fish or small animals are also cause for suspicion.



4. If you see signs of a chemical attack, quickly try to define the impacted area or where the chemical is coming from, if possible.



5. Take immediate action to get away from any sign of a chemical attack.



6. If the chemical is inside a building where you are, try to get out of the building without passing through the contaminated area, if possible.

Figure 4.32 Chemical threat response actions.

Internet Exercise: For a recent case of ricin contamination at a South Carolina postal facility, see <http://www.cdc.gov/nceh/hsb/chemicals/pdfs/mmwr5246p1129.pdf>.

4.3.2.4.2 Nerve Agents

Chemicals can also influence, in an extremely negative way, the central nervous system of the human body. Chemical nerve agents and gases have been around for more than a century. There are four main nerve agents: nerve agents GA (Tabun), GB (Sarin), GD (Soman), and VX are



Figure 4.33 Castor beans. (Courtesy of Minnesota Department of Health.)



Figure 4.34 A ricin exercise conducted by the U.S. Army.

manufactured compounds. The G-type agents are clear, colorless, tasteless liquids miscible in water and most organic solvents. Sarin is odorless and is the most volatile nerve agent. Tabun has a slightly fruity odor, and Soman has a slight camphor-like odor. VX is a clear, amber-colored, odorless, oily liquid. It is miscible with water and dissolves in all solvents. VX is the least volatile nerve agent. Most nerve agents were originally produced in a search for insecticides, but because of their toxicity, they were evaluated for military use.

Sarin was produced before the commencement of World War II and was primarily used as a pesticide. However, the gas was quickly valued for its capacity for use as chemical weaponry and was tested, though not used, during World War II. It has been alleged that Saddam Hussein used sarin against the Iranians in the long and very costly war between Iraq and Iran in the 1980s and early 1990s.⁴⁸ As noted above, it was delivered into a Tokyo subway by the radical terrorist cult Aum Shinrikyo (Figure 4.35), a cell that intended to install Shoko Asahara as its new savior. Asahara, who strove “to take over Japan and then the world,” according to the State Department, was arrested in May 1995 for his role in the subway attack. His trial took 8 years, from 1996 to 2004, when he was sentenced to death.



Figure 4.35 Shoko Asahara, cult leader who carried out Tokyo terrorism.

Sarin gas is a preferred method for the terrorist due to its ease of delivery. Aerosol or vapor forms are the most effective for dissemination; these can be carried by sprayers or an explosive device.

Internet Exercise: Chemical facilities, due to their stockpiles and ready availability of chemical substances, need to conduct vulnerability assessments of their facilities. DHS has published a vulnerability assessment guide at <https://www.cisa.gov/csatsite-security-plan>.

Tabun is a man-made chemical warfare agent classified as a nerve agent. Nerve agents are the most toxic and rapidly acting of the known chemical warfare agents. Tabun was originally developed as a pesticide in Germany in 1936. In a plot to kill Hitler in early 1945, Reich Minister of Armaments Albert Speer made inquiries about a certain quantity to be introduced into an airshaft in Hitler's final bunker. The deed was never carried out.

As in all other forms of nerve agents and other threats, the CDC disseminates educational literature to the professional community. Known as cards, these informational pieces lay out symptoms and responses regarding a particular agent. See the complete description of Tabun in Table 4.8.

VX is another recent nerve agent originally developed for industrial purposes but then construed to be an effective tool in chemical warfare. VX was originally developed in the United Kingdom in the early 1950s. VX is tasteless and slow to evaporate. Following the release of VX into the air, people can be exposed through skin or eye contact or inhalation. It can also be ingested through contaminated water or food (Figure 4.36).

VX, like other nerve gases, generally causes death by asphyxiation. The symptoms include

- Blurred vision
- Runny nose
- Slurred speech
- Tightness in the chest and constriction of the pupils
- Breathing difficulties, along with vomiting, drooling, urinating, and defecating
- Areflexia (loss of reflexes)
- Ataxia (lack of muscle control)—twitching and jerking

After the victim has lost control of his or her bodily functions, suffocation and convulsive spasms cause death. Atropine is an effective antidote if given in time.

Table 4.8 Tabun Card			
NERVE AGENT CAS # 77-81-6 RTECS # Counter-Terrorism Card 0002	TABUN (GA) dimethylphosphoramidocyanidic acid, ethyl ester Ethyl N,N-dimethylphosphoramidocyanidate Chemical Formula $C_5H_{11}N_2O_2P$ Molecular mass: 162.12		
Types of Hazard/Exposure	Acute Hazards/Symptoms	Prevention	First Aid/Fire Fighting
Fire	React with steam or water to produce toxic and corrosive vapors.	Contain to prevent contamination to uncontrolled areas.	Water mist, fog, foam, and CO_2 . Avoid methods that will cause splashing or spreading.
Explosion	May result in the formation of hydrogen cyanide.		
Exposure	- Liquid or vapors can be fatal. - Clothing releases agent for about 30 minutes after contact with vapor. - Contaminated surfaces present long-term contact hazard.	Do not breathe fumes. Skin contact must be avoided at all times.	Seek medical attention immediately.
Inhalation	Inhalation can cause symptoms in 2–5 minutes. Same sequence of symptoms despite the route of exposure: <i>Mild</i> - Runny nose - Tightness of the chest and breathing difficulty - Eye pain, dimness of vision and pin pointing of pupils (miosis) - Difficulty in breathing and cough		

(Continued)

Table 4.8 (Continued) Tabun Card

NERVE AGENT CAS # 77-81-6 RTECS # Counter-Terrorism Card 0002	TABUN (GA) dimethylphosphoramidocyanidic acid, ethyl ester Ethyl N,N-dimethylphosphoramidocyanidate Chemical Formula $C_5H_{11}N_2O_2P$ Molecular mass: 162.12		
Types of Hazard/ Exposure	Acute Hazards/Symptoms	Prevention	First Aid/Fire Fighting
	<i>Moderate</i> - Increased eye symptoms with blurred vision - Drooling and excessive sweating - Severe nasal congestion - Increased tightness of the chest and breathing difficulty - Nausea, vomiting, diarrhea, and cramps - Generalized weakness, twitching of large muscle groups - Headache, confusion, and drowsiness <i>Severe</i> - Involuntary defecation and urination - Very copious secretions - Twitching, jerking, staggering, and convulsions - Cessation of breathing, loss of consciousness, coma, and death.	Hold breath until respiratory protective mask is donned. Fire-fighting personnel should wear full protective clothing and respiratory protection during fire-fighting and rescue. Positive pressure, full face piece, NIOSH-approved self-contained breathing apparatus (SCBA) will be worn.	- If severe signs, immediately administer, in rapid succession, all three Nerve Agent Antidote Kit(s), Mark I injectors (or atropine if directed by a physician). - If signs and symptoms are progressing, use injectors at 5–20 minute intervals. (No more than three injections unless directed by medical personnel.) - Maintain record of all injections given. - Give artificial respiration if breathing has stopped. Use mouth-to-mouth when mask-bag or oxygen delivery systems not available. Do not use mouth-to-mouth if face is contaminated. - Administer oxygen if breathing is difficult.

(Continued)

Table 4.8 (Continued) Tabun Card			
NERVE AGENT CAS # 77-81-6 RTECS # Counter-Terrorism Card 0002	TABUN (GA) dimethylphosphoramidocyanidic acid, ethyl ester Ethyl N,N-dimethylphosphoramidocyanidate Chemical Formula $C_5H_{11}N_2O_2P$ Molecular mass: 162.12		
Types of Hazard/Exposure	Acute Hazards/Symptoms	Prevention	First Aid/Fire Fighting
Skin	See Inhalation Lethal doses can kill in 1–2 hours. Pupil size may range from normal to moderately reduced.	Protective Gloves: Butyl Rubber Glove M3 and M4 Norton, Chemical Protective Glove Set	The primary mode for decontamination of chemical agents is soap and water. A 0.5% hypochlorite solution can be used. There are differing guidelines for decontamination, and more research is needed to identify the optimal decontamination method. See “Personal Decontamination” and “Appendix D” in Treatment of Chemical Agent Casualties and Conventional Military Chemical Injuries (from the U.S. Navy Counterproliferation Office). See also the Medical Management of Chemical Casualties Handbook (from the U.S. Army Medical Research Institute of Chemical Defense [USAMRICD]) for a general review of the issues and more on the military decontamination powder approach.

(Continued)

Table 4.8 (Continued) Tabun Card			
NERVE AGENT CAS # 77-81-6 RTECS # Counter-Terrorism Card 0002	TABUN (GA) dimethylphosphoramidocyanidic acid, ethyl ester Ethyl N,N-dimethylphosphoramidocyanidate Chemical Formula $C_5H_{11}N_2O_2P$ Molecular mass: 162.12		
Types of Hazard/Exposure	Acute Hazards/Symptoms	Prevention	First Aid/Fire Fighting
Eyes	See Inhalation Very rapid onset of symptoms (less than 2–3 minutes).	Chemical goggles and face shield.	Immediately flush eyes with water for 10–15 minutes, then don respiratory protective mask.
Ingestion	See Inhalation Pupil size may range from normal to moderately reduced.		Do not induce vomiting. First symptoms are likely to be gastrointestinal. Immediately administer Nerve Agent Antidote Kit, Mark I.



Figure 4.36 VX gas stored on pallets. (Courtesy of the U.S. Army.)

Soman also qualifies under the definition of nerve agent. Soman was originally developed as an insecticide in Germany in 1944. Soman is commonly referred to as GD. It becomes a vapor if heated. Soman is not found naturally in the environment. Soman, like other nerve agents, can be disseminated by air, touch, or contaminated food or water. The most likely method of transmission is for people to breathe air containing Soman gas or droplets, or when the liquid form of Soman comes into contact with the skin or eyes. Because Soman mixes easily with water, it has the potential to be used as a poison for food and water supplies. Clothing from a contaminated person can release vapors for about 30 minutes after exposure, thus endangering people who were not in an original area of release.

Exposure to Soman can be treated with specific antidotes—atropine and pralidoxime chloride (2-PAM)—along with supportive medical care in a hospital. These nerve agent antidotes are most effective when given within minutes of exposure.

4.3.2.5 Improvised Explosive Devices

In addition to WMD and potential weapons of mass effect, there is the threat of terrorist attack by means of an improvised explosive device (IED). IED weapons are explosive devices fashioned and deployed by means other than through conventional military operations—thus the term *improvised*. They can be created from traditional explosive devices such as bombs, warheads, grenades, or land mines or otherwise fashioned from explosive raw materials. Ball bearings, nails, metal filings, and other materials can be utilized as damage-causing projectiles.⁴⁹ Detonation can be accomplished by wired means or remotely through a rigged cell phone, handheld device, or other wireless technology. See Figure 4.37.⁵⁰



Figure 4.37 Improvised Explosive Device (IED) components.

FBI Improvised Explosive Threat Card	
HYDROCARBONS Gas Diesel (FO) Kerosene Naphtha Carbon Black Charcoal Sugar Wax / Paraffin Vaseline Dextrin Shellac Rosin Sawdust Alcohol Ethylene Glycol	 ENERGETIC HYDROCARBONS Nitrobenzene (NB) Nitromethane (NM) Nitrocellulose (NC)
	ELEMENTAL "HOT" FUELS Powdered Metals Aluminum (Al) Magnesium (Mg) Magnalium (Mg / Al - 50/50) Zirconium (Zr) Copper (Cu) Phosphorus (P) Sulfur (S) Antimony Trisulfide (Sb₂S₃) 
Fuels consist of anything that can readily react with oxygen in a manner which produces heat. Elemental fuels can create very sensitive mixtures when mixed with oxidizers.	

Figure 4.38 IED fuels.

The fuel to ignite the IED can be common products such as “drain openers, sulfuric acid, and car batteries.”⁵¹ The Federal Bureau of Investigation (FBI) disseminates an IED threat card that categorizes the various products, compounds, and chemicals common to IEDs (see Figure 4.38).⁵²

The methods of IED delivery will vary depending on the target as well as the IED design. The Consortium of National Academies, including Science, Engineering, Medicine, and the National Research Council, charts the variety in Figure 4.39.

An inordinately high number of incidents of IED attack globally over the last several years have occurred in Iraq and Afghanistan, in addition to attacks in a number of other countries

Threat	Threat Description	Explosive Capacity	Building Evacuation Distance	Outdoor Evacuation Distance
	Small Package/letter	1 lb	40 ft	900 ft
	Pipe Bomb	5 lb	70 ft	1,200 ft
	FedEx Package	10 lb	90 ft	1,080 ft
	Vest/Container Bombs	20 lb	110 ft	1,700 ft
	Parcel Package	50 lb	150 ft	1,850 ft
	Compact Car	500 lb	320 ft	1,900 ft
	Full Size Car/Minivan	1,000 lb	400 ft	2,400 ft
	Van/SUV/Pickup Truck	4,000 lb	640 ft	3,800 ft
	Delivery Truck	10,000 lb	860 ft	5,100 ft

Figure 4.39 Various methods of IED delivery and their possible impacts. Courtesy U.S. Technical Support Working Group (TSWG).

that have begun to experience increased terrorist attacks firsthand. Unfortunately, there exist numerous online terrorist organization websites and sources that provide detailed instructions, including videos, on how to construct and deploy bombs. Often, new sites crop up as quickly as sites can be discovered and deactivated by the authorities. What is clear is that the IED phenomena, rarely if ever, is driven by singular authority. The IED campaign is a threat system that depends on a diversity of interests, parties, funding sources, and ideological support groups. The threat is far greater than the device itself. See Figure 4.40.⁵³

IED attacks have given rise to other means and related classifications of attack. Multiple IEDs can be strung together to create a “daisy chain” whereupon multiple devices can be discharged, either at once or concurrently, with a single signal. Other means of attack include a vehicle-borne improvised explosive device (VBIED), a suicide vehicle-borne improvised explosive device

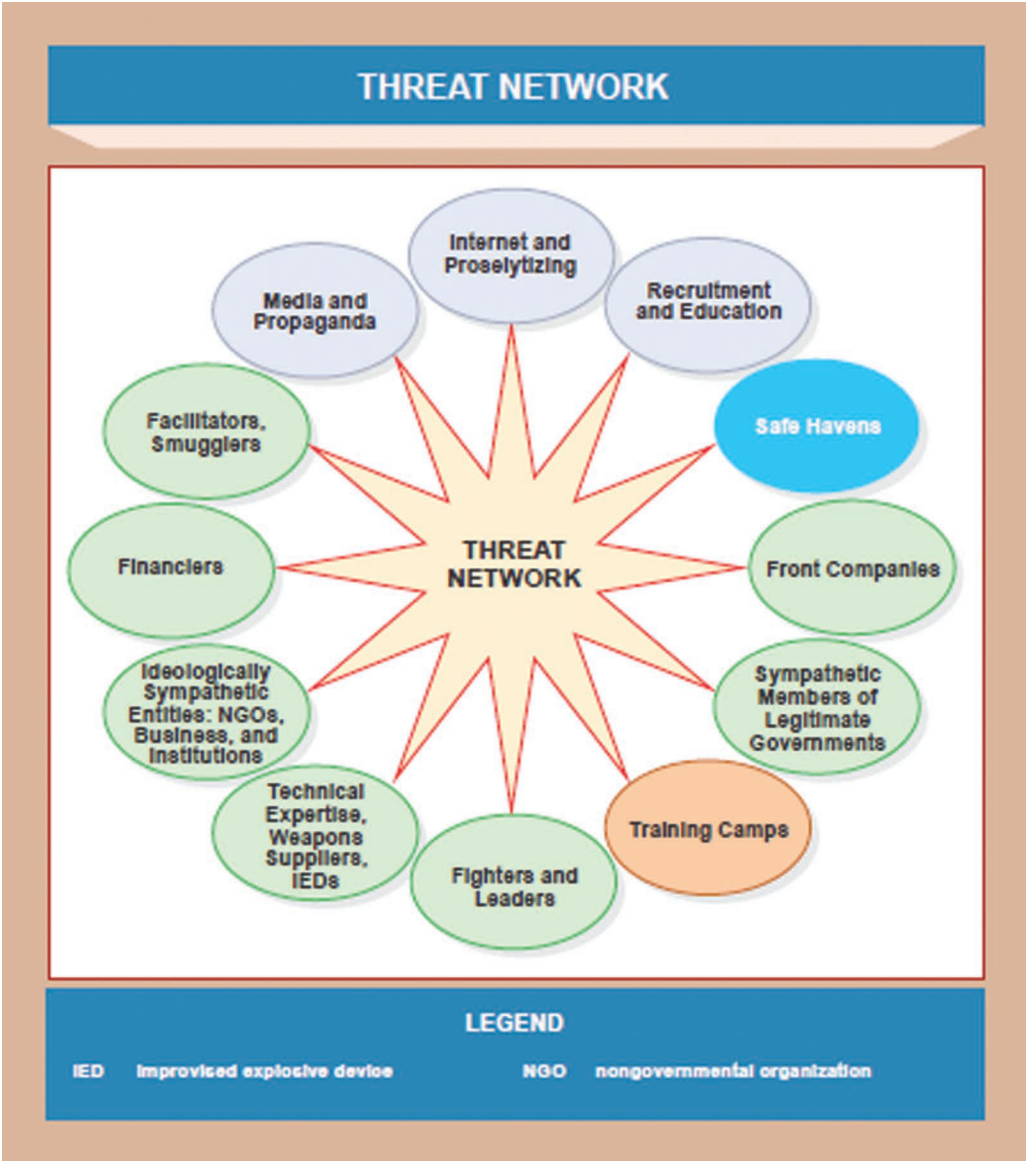


Figure 4.40 Diagram of terrorism threat components.

(SVBIED), and a suicide pedestrian-borne improvised explosive device (SPBIED).⁵⁴ Either way, the results are often physically devastating. Health impacts are immediate when in proximity to an IED and include

- Overpressure damage to the lungs, ears, abdomen, and other pressure-sensitive organs. Blast lung injury, a condition caused by the extreme pressure of an explosion, is the leading cause of illness and death for initial survivors of an explosion.
- Fragmentation injuries caused by projectiles thrown by the blast—material from the bomb, shrapnel, or flying debris that penetrates the body and causes damage.
- Impact injuries caused when the blast throws a victim into another object, that is, fractures, amputation, and trauma to the head and neck.
- Thermal injuries caused by burns to the skin, mouth, sinuses, and lungs.
- Other injuries including exposure to toxic substances, crush injuries, and aggravation of pre-existing conditions (asthma, congestive heart failure, etc.).

Timothy McVeigh carried out a VBIED attack in the case of the Oklahoma City bombing in 1995. A waterborne SVBIED attack method was utilized in the bombing of the USS *Cole* in 2000. It can be argued that the 9/11 attacks were the largest ever SVBIED attack carried out, with the jet fuel on board the planes serving as the explosive material. A series of SBIED attacks were carried out in perpetrating the London bombings of July 7, 2005. Just as tragically, the Metrojet crashing over the Sinai in Egypt on October 31, 2015, for which Islamic State in Iraq and Syria (ISIS) takes credit, appears to have relied on inside employees of the airline sympathetic to ISIS.⁵⁵

While generally smaller in scale than WMD attacks, the various IED attack methods pose an increasingly real and challenging threat in the United States and particularly to interests globally. In addition, the acquisition of bomb-making materials and the delivery and discharge of the weapon is generally far easier than with WMD weapons, and the effects are certainly just as deadly. The Paris attacks predominantly relied on AK-47 weaponry and yet the results were devastating. As a counter to this threat, military and law enforcement entities are increasingly relying upon robotic technology to seek out and destroy the destructive IED. While the human element in IED discovery will never fully disappear, the robot will assume more and more of the functions relating to detection and eventual destruction.⁵⁶ See Figure 4.41.⁵⁷

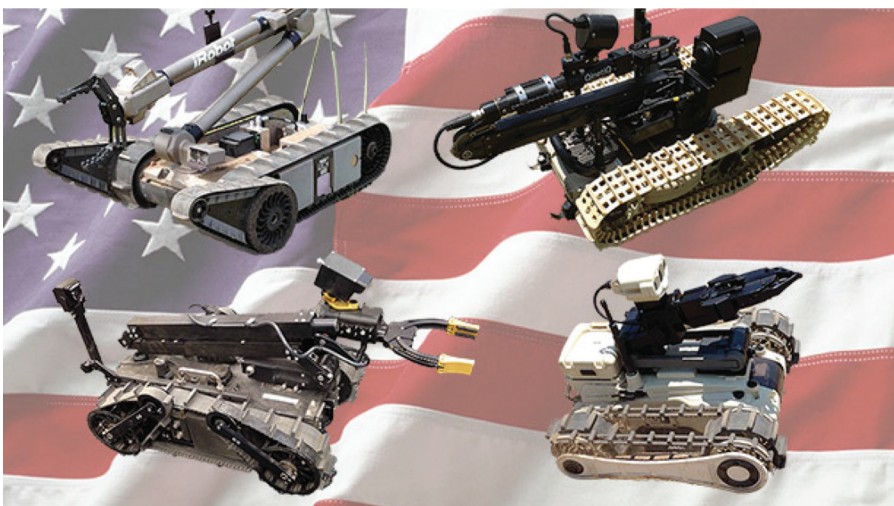


Figure 4.41 IED robots.

Homeland Security

The level of harm caused by IED attacks will also depend on its delivery location. A deserted road is a very different setting than a mass transit station. Terrorists are always looking for the maximum effect possible.

4.4 Computer Security and Information Infrastructure

The cyber world presents its own array of security challenges, and not to be forgotten is that the terrorists know that damage to the national cyber system can be devastating. Cyberspace has been defined as “the independent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical Industries.”⁵⁸

From a terrorist perspective, the virtual world provides a host of avenues of attack. From their vantage point, terrorists see a world of opportunity—the disruption of essential systems, the ruination of data and protection systems, the destruction of finance and banking, and the chance to destroy and disrupt on a major scale. Security in the virtual world should not be taken lightly. In essence, the computer system is nothing less than information infrastructure—as legitimate and likely a target for the terrorist as a bridge or water-treatment center. The information infrastructure, including government, educational institutions, and research centers as well as business and industry, is rich in potential damage. DHS and other federal agencies continuously plan for cyber threats.⁵⁹

Additionally, the cyber target often involves an economic interest or asset. To dismantle and destroy an economic system is simply another approach to warfare and conquer. Cyber teams, at both the public and private sector level, need to defend economic value and interests, and DHS dedicates a portion of its resources to doing just that. Known as CYRIE—Cyber Risk Economics, the arm of DHS dedicates itself to:

- Investment into cybersecurity controls (technology, regulatory, and legal) by private-sector, government, and private actors;
- Impact of investment on the probability, severity, and consequences of actual risks and resulting cost and harm;
- Value of the correlation between business performance measures and evaluations of cybersecurity investments and impacts; and
- Incentives to optimize the investments, impacts, and value basis of cyber-risk management. See Figure 4.42.⁶⁰



Figure 4.42 A diagram of cyber risk economics.

4.4 Computer Security and Information Infrastructure

Terrorists will target U.S. corporations, facilities, personnel, information, or computer, cable, satellite, or telecommunications systems—all of which are part of the information infrastructure. The possibilities are limitless and can include

- Denial or disruption of computer, cable, satellite, or telecommunications services
- Unauthorized monitoring of computer, cable, satellite, or telecommunications systems
- Unauthorized disclosure of proprietary or classified information stored within or communicated through computer, cable, satellite, or telecommunications systems
- Unauthorized modification or destruction of computer programming codes, computer network databases, stored information, or computer capabilities
- Manipulation of computer, cable, satellite, or telecommunications services resulting in fraud, financial loss, or other federal criminal violations⁶¹

Internet Exercise: For a full listing of potential avenues of harm in the virtual world, visit the US-CISA reading room at <https://us-cert.cisa.gov/security-publications>.

Of novel interest is how drones and other robotic devices are being utilized to hack into data systems at the institutional level.⁶²

Figure 4.43⁶³ portrays how drones can be strategically positioned to accomplish this goal.

So serious and continuous are the threats to our cybersecurity structure that in the early days of DHS's formation, there was a keen recognition that a unit dedicated to this protection would be necessary. The United States Computer Emergency Readiness Team (US-CERT) was designated as that unit. US-CERT is responsible for the management, defense, and mitigation of cyber-attacks for the federal government. To get some sense of just how extensive and continuous these threats to the cyber world are, review the reportable, high-level threats, for 1 week, as catalogued by US-CERT.

Internet Exercise: Browse the US-CERT bulletin for the week of November 9, 2015, at <https://www.us-cert.gov/ncas/bulletins/SB15-320>.

Threats can be categorized as shown in Table 4.9.⁶⁴

The US-CERT program is expected to advance information sharing among all agencies dedicated to the defense of the homeland. Its overall mission can be summarized as

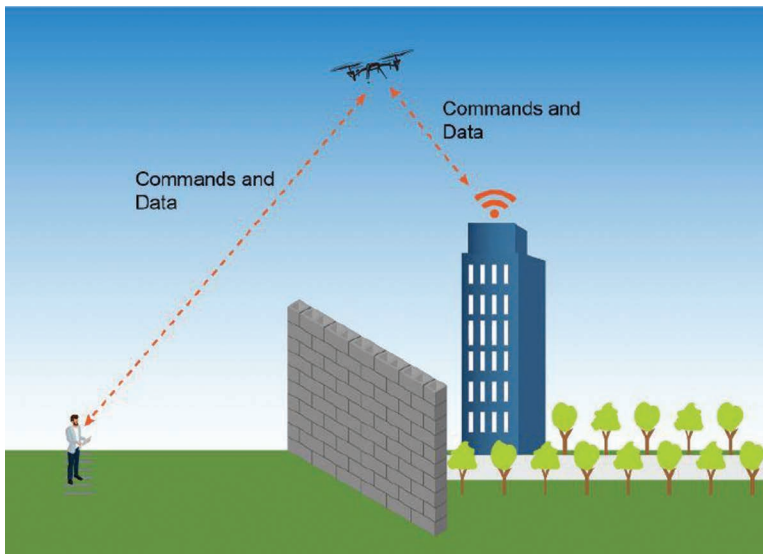


Figure 4.43 Illustration of drone usage for potential hacking purposes.

Table 4.9 Cybersecurity Threats

Threat	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the CIA, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals or small groups who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).

(Continued)

Table 4.9 (Continued) Cybersecurity Threats	
Threat	Description
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

- Providing support to national and international public and private sectors
- Event monitoring, predictive analysis, and aligned reporting tools
- Providing advance warnings regarding emerging threats
- Providing incident response for national agencies, malware analysis, and recovery support
- Involvement in national and international exercises

Threats of every sort and variety are vulnerabilities to both software and hardware. US-CERT defines cyber threats by using six distinct categories, as shown in Table 4.10.⁶⁵

Table 4.10 US-CERT Federal Agency Incident Categories			
Category	Name	Description	Reporting Time Frame
CAT 0	Exercise/network defense testing	This category is used during state, federal, national, and international exercises and approved activity testing of internal/external network defenses or responses.	Not applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized access	In this category, an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.	Within 1 hour of discovery/detection.
CAT 2	Denial of service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within 2 hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.

(Continued)

Table 4.10 US-CERT Federal Agency Incident Categories

Category	Name	Description	Reporting Time Frame
CAT 3	Malicious code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus (AV) software.	Daily note: within 1 hour of discovery/ detection if widespread across agency.
CAT 4	Improper usage	A person violates acceptable computing use policies.	Weekly.
CAT 5	Scans/ probes/ attempted access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly note: if system is classified, report within 1 hour of discovery.
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

The National Strategy to Secure Cyberspace delineates the challenges of the cyber world in the world of terrorism. Security will depend on mastery of the following tasks:

- Establishing a public–private architecture for responding to national-level cyber incidents
- Providing for the development of tactical and strategic analysis of cyber-attacks and vulnerability assessments
- Encouraging the development of a private sector capability to share a synoptic view of the health of cyberspace
- Expanding the Cyber Warning and Information Network to support the role of DHS in coordinating crisis management for cyberspace security
- Improving National Incident Management Systems (NIMS)
- Coordinating processes for voluntary participation in the development of national public–private continuity and contingency plans
- Exercising cybersecurity continuity plans for federal systems
- Improving and enhancing public–private information sharing involving cyber-attacks, threats, and vulnerabilities⁶⁶

The author of these threats is not always discernible. What is clear has been the dramatic increase in every type of vulnerability that attacks systems and software. Carnegie Mellon University

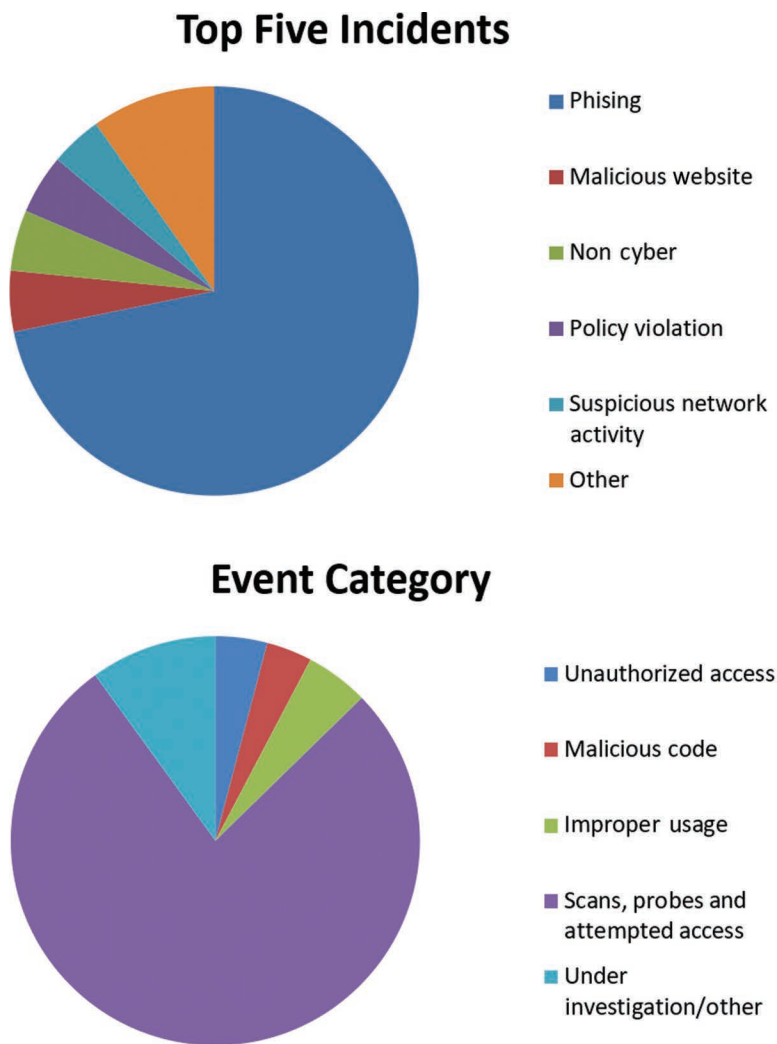


Figure 4.44 CERT vulnerabilities reported and incidents handled.

operates a Computer Emergency Readiness Team (CERT), and its statistics tracking vulnerabilities show a steady and dramatic rise of these intrusions. From 1995 to 2002, the increase has been quite marked, from 1,090 to over 4,100⁶⁷ (see Figure 4.44).

Each cyber threat displays an uncanny knack to change and alter to avoid detection, while newer versions of similar threats make detection an impossibility. The challenge of keeping up with swiftly changing technology cannot be emphasized enough.⁶⁸ To illustrate the trends, dramatic increases are shown in the growth of malware since the early 1990s (see Figure 4.45).⁶⁹

4.4.1 Cyber Challenges and the American Electoral Process

One would have to had lived in a cave or under a rock to have not been subjected to the calls of Russian influence and anomalies in the 2016 election of Donald J. Trump, both in the immediate and longer-scale aftermath. As a matter of course, Russia has long engaged in disinformation, in attempted hacking, and in general undermining of our voting process.

In response, the preparation ramping up to secure the 2020 election was one of the most concerted and coordinated efforts in history. In fact, despite claims by President Trump and his

Homeland Security

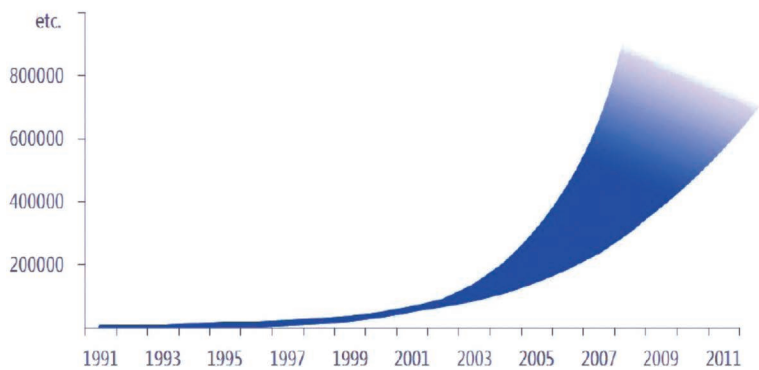


Figure 4.45 Approximate growth of malware since 1991.



Figure 4.46 CISA Director Chris Krebs from an October 2020 CISA video addressing voters regarding the 2020 Election and election security.

campaign that the election was “rigged” and marred by “massive improprieties and fraud,” the election that resulted in Joe Biden and Kamala Harris’s winning the Electoral college was said to be “the most secure in American history,” per the CISA Director at the time, Chris Krebs (see Figure 4.46).

Despite the political machinations, there is real and bona fide concern that our elective process, today so heavily reliant on touchscreen and software modalities, could in fact be hacked or tampered with. Even so, the bulk of election fraud cases, which are an incredibly small number across regional and national elections, deal with absentee ballots or with vote count manipulation.⁷⁰

Internet Resource: Find out about the real cases of voter fraud by visiting the Heritage Foundation at: <https://www.heritage.org/voterfraud>

4.4.2 National Cyber Security Division

DHS erected the National Cyber Security Division (NCSD) to be the chief DHS entity setting policy for cyber threats and the protection of cyber assets. The NCSD seeks to protect the critical cyber infrastructure 24 hours a day, 7 days a week. NCSD has identified these fundamental objectives:

- To build and maintain an effective national cyberspace response system
- To implement a cyber-risk management program for the protection of critical infrastructure

4.4 Computer Security and Information Infrastructure

NCSD, in order to give operational meaning to the National Strategy to Secure Cyberspace, established the National Cyberspace Response System. The National Cyberspace Response System coordinates the cyber leadership, processes, and protocols that will determine when and what actions need to be taken as cyber incidents arise. The Cyberspace Response System tackles other projects as well, such as

- *Cybersecurity preparedness and the National Cyber Alert System*—an information and alert system that warns of vulnerabilities.
- *US-CERT operations*—US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber-threat warning information, and coordinating incident response activities.
- *National Cyber Response Coordination Group*—made up of 13 federal agencies, this is the principal federal agency mechanism for cyber-incident response.
- *Cyber cop portal*—coordination with law enforcement helps capture and convict those responsible for cyber-attacks.
- *Cyber risk management*—assesses risk, prioritizes resources, and executes protective measures critical to securing our cyber infrastructure.
- *Cyber exercises*—Cyber Storm is a nationwide cybersecurity exercise series that takes place every 2 years. Cyber Storm was DHS's first cyber exercise, testing response across the private sector and public agencies.

4.4.3 US-CERT: Computer Emergency Response Team

That virtual security poses similar challenges to physical threats has not been lost on our nation's leaders in homeland security. Even in 2003, Homeland Security Presidential Directive 7 proclaimed that critical infrastructure includes much more than highways and transportation systems—that it just as rightfully includes the physical, virtual, and technological. America's open and technologically complex society includes a wide array of critical infrastructures and key resources that are potential terrorist targets. The majority of these are owned and operated by the private sector and state or local governments. These critical infrastructures and key resources are both physically and virtually based and span all sectors of the economy.⁷¹

In the National Strategy to Secure Cyberspace, the designation of infrastructure relating to cyberspace could not have been clearer:

Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.⁷²

At DHS, the recognition that the virtual world was a critical component of our infrastructure was adopted head on. With the implementation of the US-CERT department, the agency made plain its prioritization in the virtual world. The US-CERT is a partnership between DHS and the public and private sectors. US-CERT is the operational arm of the NCSD at DHS (Figure 4.47).

The NCSD was established by DHS to serve as the federal government's cornerstone for cybersecurity coordination and preparedness. Established in 2003, it is charged with protecting the Internet infrastructure of the United States by coordinating defense against and response to cyber-attacks. US-CERT is responsible for

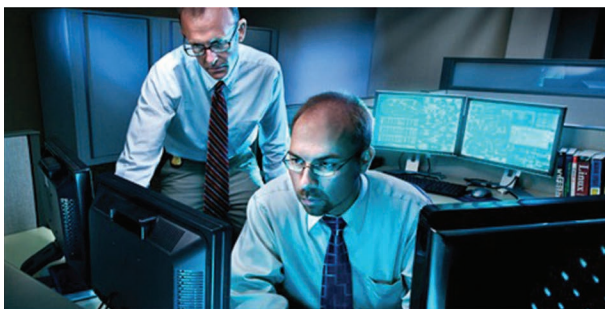


Figure 4.47 FBI cyber agents at work. (www.fbi.gov.)

- Analyzing and reducing cyber threats and vulnerabilities
- Disseminating cyber-threat warning information
- Coordinating incident response activities

US-CERT depends on the cooperative endeavors of other federal agencies, industry, the research community, state and local governments, and premier companies such as Apple and Microsoft and regular contributors to their protection program.

US-CERT provides a reporting mechanism in the event of a threat or an assault on the computer infrastructure. The reporting should not be for technical malfunction, nor should the error or problem in hardware and software be construed as unfounded or illegal. US-CERT lays out some general parameters for what types of events may qualify for reporting:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information (PII)-related incidents
- Unwanted disruption or denial of service
- The unauthorized use of a system for processing or storing data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

If the violation fits this schema, the intrusion should be reported (see Figure 4.48).

Internet Exercise: Visit the National Vulnerability Center at <http://nvd.nist.gov/>.

US-CERT was expected to be the facilitator of communication between the diverse agencies of homeland security. Part of the 9/11 critique was the lack of communication between police and fire, state and local, federal, state and local, to list just a few disconnects. US-CERT has to deal with “the various network architectures” of competing and even incompatible systems.⁷³ In addition, intelligence agencies do not naturally and easily share sensitive data and some agencies “lack access to classified networks.”⁷⁴ US-CERT is required to compile and analyze information on cybersecurity incidents and to share it with diverse constituencies. US-CERT “disseminates reasoned and actionable cybersecurity information to the public; and facilitates information sharing with state and local government, industry, and international partners.”⁷⁵

A recent Office of the Inspector General (OIG) assessment shows that US-CERT is clearly struggling to reach this mandate. The OIG is quite cognizant of the compatibility problems and other issues but makes plain that the department is really faltering on this responsibility despite earnest efforts at a sophisticated program called *Einstein*. Einstein collects network flow information and observes and identifies malicious activity in the computer network traffic. Newer versions of Einstein automatically detect intrusions and then automatically alert US-CERT to the presence of these threats. See Figure 4.49⁷⁶ for a schematic of the Einstein process and method.

4.4 Computer Security and Information Infrastructure

Section: Reporter's Contact Information	
First Name <i>(Required)</i>	
Last Name <i>(Required)</i>	
Email Address <i>(Required)</i>	
Telephone number	
<i>(Required)</i>	
Are you reporting as part of an Information Sharing and Analysis Center (ISAC)?	No, this is not an ISAC report
What type of organization is reporting this incident? <i>(Required)</i>	Please select
What is the impact to the reporting organization? <i>(Required)</i>	Please select
What type of followup action are you requesting at this time? <i>(Required)</i>	Please select
Describe the current status or resolution of this incident. <i>(Required)</i>	Please select
From what time zone are you making this report? <i>(Required)</i>	Please select a time zone
What is the approx time the incident started? (localtime)	August 21, 2008 22:20
When was this incident detected? (localtime)	August 21, 2008 22:20

Section: Incident Details

Please provide a short description of the incident and impact <i>(Required)</i>	
How many systems are impacted by this incident? (Leave blank if Unknown)	
How many sites are impacted by this incident? (Leave blank if Unknown)	
Was the data involved in this incident encrypted?	N/A
Was critical infrastructure impacted by this incident?	N/A
What was the primary method used to identify the incident	Unknown
If available, please include 5-10 lines of time-stamped logs in plain ASCII text. (e.g., CSV).	

Figure 4.48 Cybersecurity intrusion report form.

Homeland Security

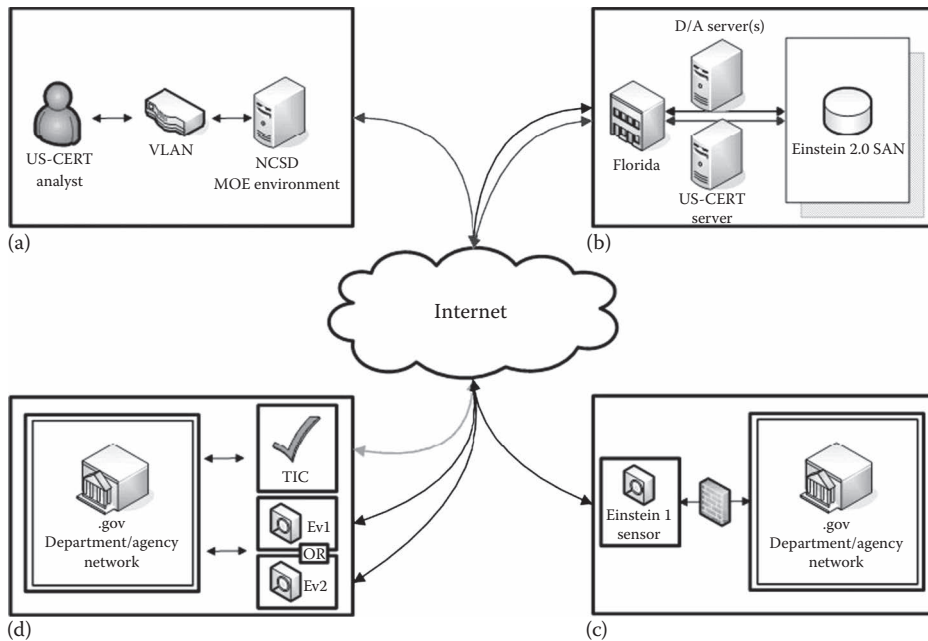


Figure 4.49 Einstein data collection infrastructure and process.

The OIG notes that while on paper these software approaches seem sensible, their operational reliability is less than sterling. It is clear the task of full integration in the world of cyber systems will be a generational undertaking.⁷⁷

4.5 Private Sector and Homeland Security

How the private sector contributes to the fight against terrorism is a story worth telling. Since 9/11, governmental agencies have urged the participation of not only state and local governments but also the active input and involvement of the general citizenry.⁷⁸ On top of this, there has been a continuous push for private business and commercial entities to be involved and an expectation that much of the American economy would need to be active players in the fight against terrorism. For example, America's chemical, water, utility, and nuclear sectors would have to be aggressively involved in the defense of their facilities and thus of the country itself.⁷⁹ Commercial interests could not simply wait for the government to do it all but instead had to jump into the mix of deterrence and prevention of terror. Infrastructure is largely owned by private enterprise and is in need of a homeland defense plan. "Industries must plan to respond...and undertake recovery under severe conditions where much of the infrastructure of the surrounding area is unavailable and site access is limited."⁸⁰ Preparedness is an industrial and commercial concern. And it is also the private citizen that encompasses the private sector. The question of how much more prepared private homes and families are has yet to be fully measured.⁸¹

Each facet of the private sector needs to understand

- How communities are impacted by terrorism
- How to create a plan of response consistent with state and federal standards
- How to mitigate loss in the event of catastrophe and disaster
- How to be active partners in the development of homeland policy

4.5 Private Sector and Homeland Security

- How to work closely with public agencies
- How to add new programs in traditional Neighborhood Watch programs that focus on terrorism⁸²

The National Infrastructure Advisory Council, in its report on public–private sector intelligence coordination, identified 17 business and commercial sectors that need to step up in the fight against terrorism:

- Communications
- Chemical and hazardous materials
- Commercial facilities
- Dams
- Defense industrial base
- Energy
- Emergency services
- Financial services
- Food and agriculture
- Government facilities
- Information technology
- National monuments and icons
- Nuclear power plants
- Postal and shipping
- Public health and health care
- Transportation
- Water⁸³

On a second front, the role of private-sector security firms and personnel can only be described as significant. The private-sector portion of criminal justice operations grows at an almost immeasurable clip.⁸⁴ According to the Homeland Security Research Corporation, by 2011, the private sector “will trail only DHS in HLS industry procurement volume. This stems from the forecasted 50% private sector procurement growth from 2007 to 2011, totaling an accumulated \$28.5B.”⁸⁵ While there have been some slight pauses in that growth, the trend for private sector and DHS partnering is onward and upward according to the Homeland Security Research Council (see Figure 4.50).⁸⁶

The face of private-sector justice can be discovered across the DHS spectrum; from privatized forces seeking out terrorists in Iraq and Afghanistan to the protection of federal installations across the mainland, private-sector justice makes extraordinary contributions in the defense of the country (Figure 4.51).⁸⁷

From Iraq to the local water facility, private-sector justice operatives are engaged in a host of activities once exclusively reserved for the public sector. This trend, often labeled “privatization,” assumes that the private sector, with its usual efficiencies and profit motivations, will carry out its task with greater effectiveness. Unions and entrenched government bureaucracies tend to be on the defensive with those promoting privatization. Those seeking greater accountability and freedom of operation tend to the privatized.⁸⁸ On paper, the concept is attractive, and in many cases, it is clear that the private sector can do a better job than the government in ensuring safety and security.⁸⁹ It will all depend on the subject matter of that security and the corresponding

Homeland Security

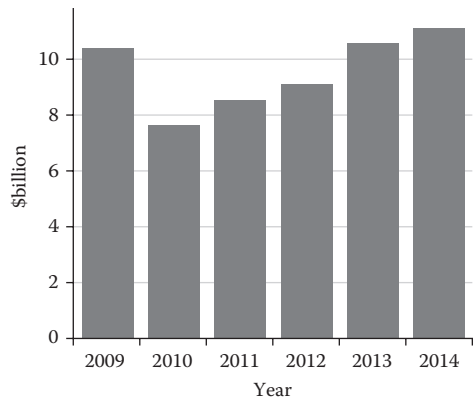


Figure 4.50 U.S. private sector homeland security market.



Figure 4.51 Private sector security personnel with Iraqi citizens.

costs. To illustrate, there are some who have argued that the Transportation Security Agency (TSA) should never have been invented and that these same services should be subcontracted to private business. Of course, this is the model pre-9/11. Since 9/11, there has been a continuous debate over the preferability of public or private in the delivery of security services. What can be agreed on is that both domains have essential responsibilities in combating terrorism—some exclusive, though most shared.

Internet Exercise: To see how private security’s premier professional association, the American Society for Industrial Security (ASIS) gets involved in the standards and practices of homeland security, see <https://www.asisonline.org/Standards-Guidelines/Standards/published/Pages/default.aspx>.

In this sense, private sector justice is driven by bottom-line considerations more than its governmental counterpart. It is motivated by efficiencies never weighed or evaluated in the public sector. And given this general motivation to the profit mentality, there are those who critique it as being willing to cut corners so that the bottom line will be brighter. Quality allegedly suffers. Indeed, many are suspicious of the qualifications of those entrusted with security responsibilities from the private sector. Do recent attempts to increase qualification and conduct legitimate background investigations on security officer applicants calm frayed

nerves?⁹⁰ Ian Patrick McGinley, when critiquing federal legislation to ensure suitable licensure and background requirements for security officers, found that the industry is in a state of market failure.

Nevertheless, significant problems with leaving regulation to the market make this option unfeasible. For one, despite laudable attempts, the industry's self-regulation track record has been poor. Second, profit margins in the security industry are tight because many companies view security as a necessary evil. As a result, there is a race to the bottom—in terms of pricing and salaries—in order to gain a competitive advantage relative to other firms, resulting in less qualified officers.⁹¹

However, this argument does not pan out in so many governmentally operated entities. What of the public-school system nationally? Are these systems not in crisis? What of public transportation systems? What of roads and bridges in near collapse? It is not difficult to discern where government fails to meet its mission. Privatization is evident everywhere—prisons, policing, and courts, to name just three, are examples of fields seeing these trends.⁹² As the Bureau of Justice Assistance notes in its *Engaging Private Security to Promote Homeland Security*, private-sector justice can jump in feet first.

Private security can

- Coordinate plans with the public sector regarding evacuation, transportation, and food services during emergencies
- Gain information from law enforcement regarding threats and crime trends
- Develop relationships so that private practitioners know whom to contact when they need help or want to report information
- Build law enforcement understanding of corporate needs (e.g., confidentiality)
- Boost law enforcement's respect for the security field

Working together, private security and law enforcement can realize impressive benefits:

- Creative problem-solving
- Increased training opportunities
- Information, data, and intelligence sharing
- Force multiplier opportunities
- Access to the community through private-sector communications technology
- Reduced recovery time following disasters⁹³

The National Defense Industrial Association (NDIA), another premier professional group for the private sector, argues as if the task of homeland security is integral to any private security firm. It unequivocally aims

- To provide legal and ethical forums for the exchange of information, ideas, and recommendations between industry and government on homeland security issues
- To promote a vigorous, robust, and collaborative government–industry homeland security team
- To advocate for best-in-class, high-technology equipment, systems, training, and support for America's first-responder community⁹⁴

And not only is it capable of carrying out its own mission in the world of homeland security, but it should do so with collaboration and collegiality in regard to its public partners. The worlds of public and private are not distinct or radically different; rather, these are compatible and

Homeland Security

complementary domains where a shared mission is obvious. Partnerships are what each should be looking for since the public and the private share 12 essential components:

- Common goals
- Common tasks
- Knowledge of participating agencies' capabilities and missions
- Well-defined projected outcomes
- A timetable
- Education for all involved
- A tangible purpose
- Clearly identified leaders
- Operational planning
- Agreement by all partners as to how the partnership will proceed
- Mutual commitment to providing necessary resources
- Assessment and reporting⁹⁵

DHS formally encourages interplay and cooperation between private-sector justice entities and the public law enforcement function. Throughout DHS policy making is the perpetual recognition that it cannot go it alone and that it needs the daily cooperation of the private sector. Within its Office of Policy, DHS has erected a Private Sector Office, its chief aims being

- To engage individual businesses, trade associations, and other nongovernmental organizations in fostering dialogue with the department
- To advise the secretary on prospective policies and regulations and, in many cases, on their economic impact
- To promote public–private partnerships and best practices to improve the nation's homeland security
- To promote department policies to the private sector

The Private Sector Office focuses on two major functions: the Business Outreach Group and the Economics Group. In the first instance, DHS affirmatively connects with the business and commercial sector, fully realizing that cooperation and joint endeavors fare better than isolation or turf protection. The Outreach Group seeks input and advice from the business sector before the institution or implementation of policy. The Outreach Group

- Meets with private-sector organizations and department components to promote public–private partnerships
- Promotes departmental policies
- Gathers private-sector perspectives for use by the department

The Economics Group weighs policy in cost–benefit terms. Here, DHS is deaf to the costs of policy implementation since each new regulation or requirement does have a corresponding price tag. As a result, the group looks at the impact of policy from various directions, including

- *Policy analysis*—it evaluates the economic impacts of departmental policies on the private sector.

4.5 Private Sector and Homeland Security

- *Process analysis*—it evaluates departmental processes that will allow the private sector to operate efficiently while meeting national security needs.
- *Regulatory analysis*—it provides a resource to the department on regulatory/economic analyses.
- *Metrics*—it promotes the use of metrics to identify successes and areas needing improvement.
- *Benefits methodology*—it actively works on the development of methodologies to quantify the benefits of homeland security investments.

The Economics Group coordinates economic roundtables and publishes white papers and other studies that highlight cost–benefit.

Internet Exercise: The DHS has recently published a full catalog of resources available to the private sector which fosters cooperation between public entities and private sector entities: See: https://www.dhs.gov/sites/default/files/publications/private_sector_resources_catalog.final_1.23.2020_0.pdf

The health of the Private Sector office also heavily depends on the active participation of the Private Security Industry—an economic juggernaut that increasingly assumes roles in the homeland defense and assurance of security. The industry has long been a major player in the research and development of technology for homeland, and DHS continuously taps the expertise of the private sector for innovation and creative applications to security problems.⁹⁶ From the industry’s point of view, the opportunities for growth in homeland matters are at the starting block with the future being bright indeed.⁹⁷ At literally every corner of the world, the private security industry has charged forward with new and innovative technologies, emerging and dynamic techniques of access control and screening as well as enhanced protective measures for people, infrastructure, and valuable assets. DHS has even structurally recognized the central role that private security and private sector interests deliver in homeland defense by the creation of an Office directly dedicated to fostering this close, collaborative association.⁹⁸

Known as the Private Sector Office (PSO), its fundamental purpose is to:

- Advises the Secretary on the impact of the Department’s policies, regulations, processes, and actions on the private sector.
- Creates and fosters strategic communications with the private sector to enhance the primary mission of the Department to protect the American homeland.
- Interfaces with other relevant Federal agencies with homeland security missions to assess the impact of these agencies on the private sector.
- Creates and manages private-sector advisory councils composed of representatives of industries and associations designated by the Secretary to: (1) Advise the Secretary on private sector products, applications, and solutions as they relate to homeland security challenges; and (2) Advise the Secretary on homeland security policies, regulations, processes, and actions that affect the participating industries and associations.
- Works with Federal laboratories, federally funded research and development centers, other federally funded organizations, academia, and the private sector to develop innovative approaches to address homeland security challenges to produce and deploy the best available technologies for homeland security missions.
- Promotes existing public–private partnerships and development of new public–private partnerships to provide for collaboration and mutual support to address homeland security challenges

Homeland Security

- Assists in the development and promotion of private-sector best practices to secure critical infrastructure.
- Coordinates industry efforts regarding department functions to identify private sector resources that could be effective in supplementing government efforts to prevent or respond to a terrorist attack.
- Consults with the various DHS elements and Department of Commerce on matters of concern to private sector including travel and tourism industries.⁹⁹

Hence, over the last 20 years managing the global and national threats of terrorism and disasters, both governmental and private resources have been employed. It has never been an all or nothing proposition but instead a joint and collaborative effort to minimize harm. Millions of private security employees are delegated to the tasks of bridges and courthouses, energy plants and nuclear plants, chemical and agricultural facilities as well as a host of other locations that perpetually need protection from threat and harm. None of this would be possible without the active and persistent participation of the private security industry.¹⁰⁰

The private security industry is fully aware of this firm relationship with the scions of homeland defense. Most security companies market and account for homeland defense services relative to the protection of critical infrastructure like parks, bridges, tunnels, and airports to name just a few. In some cases, it is only the security firm that provides this needed protection while in other cases, the delivery is partnership or jointly done. Public policing often relies on its partnership with security firms to carry out tasks and duties it cannot fully cover.

How these cooperative alliances have unfolded since 9/11 as well as how much territory has been assumed by private sector security since the first days of response to 9/11, is clearly an important piece of our homeland defense. Since the very beginning of the DHS, there has never been an exclusionary tone taken to private sector interests. In its place, the DHS historically fostered strong and viable relationships with its private partners while fully recognizing the impossibility of government alone tackling the homeland defense. In this way, examining the state of affairs over a 20-year cycle from right before the 9/11 tragedy until today. In the U.S. alone, almost half a million security guards work for NASCO member companies, by way of illustration, protecting a large number and variety of homeland assets. The larger firms, such as Allied Universal, with in excess of 200,000 employees now dedicate homeland defense in their corporate and strategic outlook. Prior to 9/11, private security—despite being three times larger than public sector law enforcement in both budget and personnel—lacked uniform standards (e.g., licenses, training, education, background checks) and state-regulated requirements to guide new and current security professionals.

After 9/11, the security industry grew to fit the market, both in personnel and technology, and changed the functions of security within the organization to include crisis management, business continuity, risk assessment, threat analysis, preparedness, response, and mitigation.¹⁰¹ Consequently, the security manager was accepted as a C-suite level partner and professional (i.e., Chief Security Officer/Chief Information Security Officer), working closely with CEOs and CFOs, aiding HR in personnel-related aspects, and serving on the Board of Directors.¹⁰² No position in private security, from the basic to the executive has remained stagnant; thus, it is necessary for the industry to understand the changes in the roles and functions private security has in serving the homeland.¹⁰³

Three aspects of private security in homeland developed and evolved after 9/11—private-public partnership, availability of security training and education programs, and technology. One of the main realizations from the 9/11 tragedy was that homeland security could not rely solely on the public sector to protect assets. Regardless of the catastrophic event source—natural hazard like a hurricane or man-made disasters, such as from terrorism or active shooting incidents—having a public-private partnership in place is the key to success, as well as mutually beneficial.¹⁰⁴ Intelligence gathering is merely the first step in identifying patterns that could aid in

thwarting disaster; both the public and private sectors must integrate this information and coordinate the necessary steps to identify and mitigate risks, strengthen preparedness, and respond to and recover from cyber and physical attacks, particularly for Critical Infrastructure and Key Resources.¹⁰⁵ Although the roles and functions of both entities have become increasingly formalized, with the private sector responsible for protecting corporate assets as part of national defense, it is still unclear how much of what private security personnel do is under sole vs. dual authority.¹⁰⁶ It would also be important to ascertain whether the current partnerships have developed communication, cooperation, coordination, and collaboration, as well as which barriers or challenges to information sharing (e.g., lack of trust) may still be preventing private-public coordination.¹⁰⁷

The sheer number of security personnel needed to protect homeland led to the realization that they, like their public sector counterparts, should have specific training and education. Following 9/11, there was growth in academic programs in Homeland Security, Private Security, and Security Management.¹⁰⁸ Low-level programs, such as trade and vocational schools, along with top-down training and professional certificate programs by various professional societies, such as ASIS, ACFE, LPF, have contributed to the security profession.¹⁰⁹ It is unknown whether these programs are meeting the needs of security personnel in terms of preparing them for their low-, middle-, and high-level positions and the continuously emerging security threats. A related aspect of education concerns professionals' capability in using rapidly developing security technology properly.¹¹⁰ Private security relies on technology for "gathering intelligence, preventing attacks and natural disasters, responding to events, and recovering from them."¹¹¹ Cyber, physical, and personnel security professionals use technology for a variety of tasks, such as detecting data irregularities and gathering intelligence, identifying criminals through facial recognition, improving communication for rescue in disasters, managing events and recovery, surveillance, limiting employee access, etc.¹¹² DHS and Law enforcement is able to take advantage of private security technology, such as CCTV in various businesses, and crime-solving and prevention technologies, such as object and behavior recognition software or radio frequency identification tagging and a host of other protocols crucial to homeland defense.

Finally, DHS, not long after 9/11, instituted an advisory committee on private-sector cooperation and collaboration. Members of the committee represent the full panoply of industry, corporate interests, and security firms with shared interests. From the outset of DHS, it was clear that policy making would not occur without the input of industry and commerce. It was equally evident that the skilled practitioners of private-sector justice would be crucial contributors.

4.6 Conclusion

Any operational notion of what homeland security is must include a look at traditional aspects of security, such as risk and threat, as well as new and emerging hazards. This chapter surveys the likely and even unlikely events that will challenge those laboring in the field of homeland security. First, how does the professional define and measure risk? What criteria and variables need to be considered when assessing risk? Are some risks worth taking and others never tolerable? Are some locations more vulnerable to risk than others? Are the costs of the risk, relative to its potential harm, worth the investment? In short, risk cannot be assessed in a vacuum but must be weighed in light of the likelihood of occurrence, costs of prevention, and the nature of the harm to be inflicted. Various systems of measurement relative to risk are also provided, including CARVER+Shock methodology.

Next, the chapter's coverage turns to the typology of threat and hazard. From natural to terrorist in design, threats and hazards must be evaluated considering the perpetrator's motivation. In the natural world, there is no malice. In the world of terrorism, the homeland professional must anticipate how far the actor will go to achieve a particular end. Hijackings, bombs, and WMD manifest a direct intentionality, while the hurricane and flood do not.

As for threats that impact the homeland security dimension, nothing is more pressing or compelling than the world of WMD. WMD are unique in many senses, especially when one considers the nature of the harm inflicted and the potentiality for widespread destruction.¹¹³

The fear and dread of a nuclear event is probably the most pronounced of any form of WMD. In particular, the chapter looks at the relative ease of delivery of various WMD by a dirty bomb mechanism. In addition, agencies such as the NRC are highlighted regarding radiological security programs. The world of bioterrorism is just as frightening, and the accessibility and general availability of bioagents should give any homeland professional cause for concern. The chapter expends considerable energy discussing anthrax, plague, and smallpox—three biological invasions that would cause both terror and widespread injury. Also covered are the diverse means to deliver and infect by chemical substance. The use of sarin gas, used as recently as 1995, indicates the extraordinary potential for harm that these agents can inflict. Biotoxins, blister agents, blood agents, acids, and other caustics, as well as respiratory agents, are all evaluated. Special coverage of ricin, Tabun, and other specific nerve agents is included.

The next portion of this chapter deals with the need to protect computer data and secured information and the equal imperative placed on information sharing between the full array of agencies involved in the homeland response. DHS fosters this approach by operating a National Cyber Alert System, where threats to computer infrastructure are catalogued and publicly announced. DHS posts a National Strategy to Secure Cyberspace, which urges both the public and private sectors to take the necessary steps to ensure continued operation of computer functions and maintenance of data integrity. Cyber threats are just as real as any other threat. The NCSD is DHS's chief arm to ensure integrity in the system. US-CERT plays a deterrence and prevention role in cyber threats and also serves as an analysis reaction team to cyber threats.

The final section reviews the collaboration of private-sector interests with the public functionality of homeland practice. Exactly how does the private sector aid in the fight against terrorism? To illustrate, the American industrial complex of utilities, chemical facilities, and manufacturing centers that produce defense products are all relevant to homeland defense. These private entities are construed as critical infrastructure in need of both plan and protection. The National Infrastructure Advisory Council highlights the need for private interests to aggressively participate in the defense of the country. Just as significant will be the rise of private sector justice operatives fighting terrorism. In Iraq, the growth of private security firms, the recognition that private soldiers now engage or protect, and the fact that private companies and firms are better suited to the reconstruction of Iraq than governmental entities are now indisputable conclusions. DHS encourages the partnership of the public with the private by and through its Private Sector Office and its Advisory Committee on the Private Sector.

Keywords

Accessibility; Analytic Risk Assessment; Anthrax; Asset Value; Biological WMD; Bioterrorism; Biotoxin; Blister Agent; Blood Agent; CARVER + Shock Assessment; Chemical WMD; Civil Hazard; Consequence; Criticality; Cyber Warning and Information Network; Cyberspace; Daisy Chain; Deliberative Risk Assessment; Dirty Bomb; Effect; Flow Process; Force-on-Force Training; Harm; Hazard; IED (Improvised Explosive Device); Information Infrastructure; National Cyber Security Division; National Cyberspace Response Team; National Vulnerability Center; Natural Hazard; Nerve Agent; Nuclear Regulatory Commission; Nuclear WMD; Pathogen; Plague; Practical Risk Assessment; Private Sector; Privatization; Public Health Risk; Public – Private Partnership; Radiological Dispersion Device; Radiological WMD; Recognizability; Recuperability; Ricin; Risk; Risk Assessment; Risk Management; Sarin; Shock; Smallpox; Soman; SPBIED (Suicide Pedestrian-Borne Improvised Explosive Device); SVBIED (Suicide Vehicle-Borne Improvised Explosive Device); Tabun; Threat; Threat Rating; US-CERT; VBIED (Vehicle-Borne Improvised Explosive Device); Vulnerability; Vulnerability Rating; VX; WMD

Discussion Questions

1. In the area of risk analysis, the question of exposure is heavily emphasized. Can you envision a circumstance when a risk that lacks significant exposure would still be considered more serious than a risk with a higher exposure?
2. Can another formula for the measure of risk be formulated?
3. Relay your view of the CARVER+Shock system of risk assessment. What are its strengths and shortcomings?
4. Some have argued that DHS should not concern itself with the world of natural hazards and threats. Comment on this school of thought.
5. It has been said that the world of WMD is highly exaggerated. How so? Can you provide an example of this hyperbole?
6. Biological terrorism is probably the easiest form of WMD to construct and deliver. Explain.
7. Chemical weaponry can be produced with easy access to products and components. Discuss.
8. Chemical weapons are not always the invention of the chemist but instead can be natural in design and makeup. Discuss.
9. Discuss the role and functions of a US-CERT team.
10. Discuss how computer networks can be designated critical infrastructure.
11. Relate three common threats to a cybersystem.
12. The role of the private sector in homeland defense continues unabated. Why do you think the privatization of homeland services will march forward with very little resistance?
13. What types of industries need the highest level of concern regarding homeland security?

Practical Exercises

1. Conduct a threat and risk assessment regarding chemical facilities in your region. Respond to the following questions:

What type of products exist?

What potential injuries can arise from these products?

What is the potential for mass destruction?

What safety and security information on the company's website addresses risk in the community?

2. Create a flowchart assessment mechanism, under the CARVER+Shock method, to measure a manufacturing threat in your area.
3. Identify nuclear facilities within 100 miles of your residence. Respond to the following:

Describe the facility.

How many people and communities does the facility serve?

In the event of a nuclear event, explain how the surrounding environs would be impacted.

Homeland Security

In what way would injury touch the largest base of people?

Discuss the facility's evacuation policy relative to the community.

4. Contact your local office dedicated to homeland security. Gather information on your area's anthrax program. Explain in two paragraphs what that plan or program is.
5. Identify and chart transportation infrastructure in your area. Respond to the following:
Which infrastructure has the capacity to inflict the most damage?
What steps are being taken to secure that infrastructure?
Despite these steps, how can a terrorist bypass the protections?
Point out specific vulnerabilities that you can identify.
6. The Emergency Management Institute publishes a bevy of very useful assessment tools. Complete the community and geography survey at <https://training.fema.gov/hiedu/needsat.aspx>.
7. Find out about FEMA's Hazus program—a risk assessment tool for natural disasters (<http://www.fema.gov/hazus-software>).
8. Visit the Cyber Storm web location and evaluate how your department or community might have responded. Provide a two- to three-page response and assessment.
9. Make a list and database for at least ten private companies that design and manufacture explosive detection equipment, scanning devices, cargo and container scanners, and other novelties in the screening of commercial goods and trade.
10. List six applications of biometrics and the companies that produce the technology.

Notes

- 1 J. C. Chicken and T. Posner, *The Philosophy of Risk* (London: Thomas Telford, 1998).
- 2 D. Dunai, A framework of cardinal directions: Threats and challenges to the United States, *AARMS Security*, 10 (2011): 327–357, at 331. See also: US Department of State, *Country Reports on Terrorism 2017*, <https://www.state.gov/reports/country-reports-on-terrorism-2017/> (accessed August, 10, 2020).
- 3 See: Central Florida Intelligence Exchange, *Jihadist Propaganda Provides Guidance for Lone Offender Attacks Against Law Enforcement*, (2014), <https://info.publicintelligence.net/CFIX-LoneJihadistAttacks.pdf> (accessed August, 10, 2020).
- 4 See: Army Threat Integration Center (ARTIC), *Special Assessment: ISIL Threats Against the Homeland* (2014), <https://info.publicintelligence.net/ARTIC-HomelandThreatsISIL.pdf> (accessed August, 10, 2020).
- 5 Federal Emergency Management Agency, *Building Design for Homeland Security* (Washington, DC: U.S. Government Printing Office, 2004), V-5.
- 6 *Ibid.*, V-6.
- 7 *Ibid.*, V-9.
- 8 H. R. Willis, *Risk Informed Resource Allocation at the Department of Homeland Security* (Santa Monica, CA: Rand Corporation, 2007), 3.
- 9 U.S. Department of Homeland Security, *Risk Analysis: Fact Sheet Series*, 2006.
- 10 USDHS, *Risk Analysis Sheet*; See also how to conduct visual inspection for vulnerability and risk in specified locations at: CISA Website, *Infrastructure Visualization Platform* page, <https://www.cisa.gov/infrastructure-visualization-platform> (accessed August 10, 2020).

- 11 D. R. Coats, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community 11 (2019), <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf> (accessed August 10, 2020).
- 12 U.S. Department of Homeland Security, Risk Analysis: Fact Sheet Series, 2006.
- 13 See: CISA Website, Infrastructure Survey Tool page, <https://www.cisa.gov/infrastructure-survey-tool> (accessed August 10, 2020).
- 14 Federal Emergency Management Agency, Mitigation Planning How-to Guide #3: Developing the Mitigation Plan (Washington, DC: U.S. Government Printing Office, April 2003), 1.
- 15 See U.S. Food and Drug Administration, CARVER+Shock Users' Manual, Version 1.0, 2007, Appendix B.
- 16 Prepared remarks by Secretary Napolitano at Harvard University's John F. Kennedy Jr. Forum, April 15, 2010, www.dhs.gov/ynews/speeches/sp_1271366935471.shtm (accessed August 10, 2020).
- 17 See: FedRAMP Security Assessment Framework, (2017), https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf (accessed August 10, 2020).
- 18 See: FedRAMP Website, About Us, <https://www.fedramp.gov/about/> (accessed August 10, 2020).
- 19 D. Dunai, A Framework, at 330.
- 20 Data from the Centre for Research on the Epidemiology of Disasters, 2015, www.cred.be.
- 21 Ibid.
- 22 See Department of Homeland Security, Science and Technology Directorate, <http://www.dhs.gov/science-and-technology/our-work> (accessed August 10, 2020); T. P. McAllister, F. Sadek, J. L. Gross, J. D. Averill, and R. G. Gann, Overview of the structural design of World Trade Center 1, 2, and 7 buildings, *Fire Technology* 49 (2013): 587; R. L. Reid, NIST: World Trade Center Building 7 is first known case of a tall building collapsing 'primarily' from fire, *Civil Engineering-ASCE* 78 (2008): 30; See also: R. J. Bunker and A. Keshavarz, Terrorist and Insurgent Teleoperated Sniper Rifles and Machine Guns, (2016), <https://info.publicintelligence.net/USArmy-TeleoperatedSniperRifles.pdf> (accessed August 10, 2020).
- 23 Army Advances Learning Capabilities of Drone Swarms, (2020), <https://info.publicintelligence.net/USArmy-TeleoperatedSniperRifles.pdf> (accessed November 24, 2020).
- 24 See: National Protection and Program Directorate, Future Environment Net Assessment: Autonomous Vehicles, (2017), https://www.army.mil/article/237978/army_advances_learning_capabilities_of_drone_swarms
- 25 Bauer, War on terror or policing terrorism? Radicalization and Expansion of the Threats, *Police Chief*, (2011): 46–52, 52.
- 26 See: New Jersey Regional Operations Intelligence Center, Intelligence Advisory: Potential Concerns for Transportation Security, 5 (March 24, 2016), <https://info.publicintelligence.net/NJROIC-TransportationSecurity.pdf> (accessed August 10, 2020).
- 27 See: J. Garamone, Military Must Be Ready to Confront Hybrid Threats, Intel Official Says, September 6, 2019, <https://www.dni.gov/index.php/newsroom/news-articles/item/2040-military-must-be-ready-to-confront-hybrid-threats-intel-official-says> (accessed August 10, 2020).
- 28 See: Inspire Magazine- a domestically produced jihadi production which outlines innovative methods and means of terror at: FBI, WMD Operations Unit 1, Second Issue of Jihadist Magazine Encourages Use of Weapons of Mass Destruction, October 15, 2010, <https://info.publicintelligence.net/FBI-InspireWMD.pdf> (accessed August 10, 2020).
- 29 See: Congressional Research Office, China and Proliferation of Weapons of Mass Destruction and Missiles: Policy Issues Shirley A. Kan Specialist in Asian Security Affairs May 26, 2011; See also: Council on Foreign Relations, China's Maritime Disputes, <https://www.cfr.org/interactives/chinas-maritime-disputes> (accessed August 10, 2020).
- 30 National Air and Space Intelligence Center, Ballistic & Cruise Missile Threat, <https://info.publicintelligence.net/NASIC-BallisticMissileThreat.pdf> (accessed August 10, 2020).
- 31 Ibid., at 9.
- 32 See Department of Homeland Security, Nuclear Reactors, Materials, and Waste Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan, 2010.
- 33 Department of Homeland Security, Nuclear Sector—Specific Plan 47, 2010.
- 34 U.S. Nuclear Regulatory Commission, Office of Nuclear, Security and Incident Response (Washington, DC: U.S. Government Printing Office, April 2005), 44.

- 35 D. G. Arce and K. Siqueira, Motivating operatives for suicide missions and conventional terrorist attacks, *Journal of Theoretical Politics* 26 (2014): 677; R. Braun and M. Genkin, Cultural resonance and the diffusion of suicide bombings: The role of collectivism, *Journal of Conflict Resolution* (2013).
- 36 FEMA, National Exercise Program (2001), http://www.fema.gov/media-library-data/20130726-1829-25045-3774/national_exercise_program_base_plan__2011_03_18_.pdf (accessed August 10, 2020).
- 37 White House Office of the Press Secretary, President Obama releases National Strategy for Countering Biological Threats, December 9, 2009, <https://obamawhitehouse.archives.gov/the-press-office/2009/12/09/president-obama-releases-national-strategy-countering-biological-threats> (accessed August 10, 2020); See also: US Government Accountability Office, BIODEFENSE: The Nation Faces Long-Standing Challenges Related to Defending Against Biological Threats, June 26, 2019, <https://www.gao.gov/products/GAO-19-635T> (accessed August 10, 2020).
- 38 Testimony of Tara O'Toole before the House Subcommittee on Homeland Security Appropriations, on Biosurveillance, April 16, 2010, Washington, DC.
- 39 Observations on the cancellation of BioWatch Gen-3 and future considerations for the program, GAO-14-267T, (June 10, 2014), <https://www.gao.gov/products/D07558> (accessed August 10, 2020).
- 40 See the National Institute of Health's list of pathogens and infectious materials, <https://www.niaid.nih.gov/topics/biodefenserelated/biodefense/pages/cata.aspx> (accessed August 10, 2020).
- 41 Centers for Disease Control and Prevention, bioterrorism agents/diseases list, <http://emergency.cdc.gov/agent/agentlist.asp> (accessed August 10, 2020).
- 42 Centers for Disease Control and Prevention, Division of Vector-Borne Diseases, Plague symptoms, <http://www.cdc.gov/plague/symptoms/index.html> (accessed August 10, 2020).
- 43 Centers for Disease Control, Smallpox Response Plan and Guidelines (Washington, DC: U.S. Government Printing Office, November 2002), Annex 8.
- 44 Ian Pannell, Syria civilians still under chemical attack, BBC News Online, September 10, 2015, <http://www.bbc.com/news/world-middle-east-34212324> (accessed August 10, 2020).
- 45 A. Üzümcü, The chemical weapons convention-disarmament, science and technology, *Analytical and Bioanalytical Chemistry* 406 (2014): 5071.
- 46 See: Federal Bureau of Investigation, FBI Bulletin: Use of Fraudulent University E-mail Accounts to Purchase Chemicals, February 27, 2014, <https://publicintelligence.net/fbi-fraudulent-chemical-purchases/> (accessed August 10, 2020).
- 47 M. Patel et al., Recognition of illness associated with exposure to chemical agents—United States, 2003, *Morbidity and Mortality Weekly Report*, 52 (October 3, 2003): 938–940, <http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5239a3.htm#tab> (accessed August 10, 2020).
- 48 The Arms Control Association makes this claim in M. Nguyen, Report confirms Iraq used Sarin in 1991, *Arms Control Today*, 36 (January/February 2006), http://www.armscontrol.org/act/2006_01-02/JANFEB-IraqSarin (accessed August 10, 2020).
- 49 H. Hogan, Identifying explosives, after the fact, *Homeland Security Today Magazine* (September 2011): 18–19.
- 50 See: US Armed Forces Joint Publication, Counter-Improvised Explosive Device Operations I-2 (2012), <http://www.bits.de/NRANEU/others/jp-doctrine/JP3-15.1%2812%29.pdf> (accessed August 10, 2020).
- 51 K. Yeager, What law enforcement needs to know about improvised explosives, *Police Chief* (September 2011): 52–55.
- 52 National Academies & Department of Homeland Security, Fact Sheet: IED Attack Improvised Explosive Devices, News & Terrorism, Communicating in a Crisis.
- 53 See: US Armed Forces Joint Publication, Counter-Improvised Explosive Device Operations II-2 (2012), <http://www.bits.de/NRANEU/others/jp-doctrine/JP3-15.1%2812%29.pdf> (accessed August 10, 2020).
- 54 See: Army/Marine Corps, Ground Robotics Master Plan (2007), <https://info.publicintelligence.net/USA-USMC-GRMP.pdf> (accessed August 10, 2020).
- 55 C. Smith, ISIS says soda can bomb detonated on Russian plane was intended for western passenger jet, November 19, 2015, <http://bgr.com/2015/11/19/isis-soda-can-bomb-airplane-metrojet-kg19268> (accessed August 10, 2020).

- 56 See: U.S. Department of Homeland Security, Small Platform Tactical Robots Assessment Report, https://www.dhs.gov/sites/default/files/publications/SPT-Robots-AR_1014-508_0.pdf (accessed August 10, 2020); See also: Teams and specialists in both civilian and military roles, will continue to play a key role in IED detection as noted in: US Army, Counter-Improvised Explosive Device Integration Cells, March 10, 2010, https://www.army.mil/article/35580/counter_improvised_explosive_device_integration_cells (accessed August 10, 2020).
- 57 See: U.S. Department of Homeland Security, Small Platform Tactical Robots Assessment Report, https://www.dhs.gov/sites/default/files/publications/SPT-Robots-AR_1014-508_0.pdf (accessed August 10, 2020).
- 58 National Security Presidential Directive 54, Cyber Security and Monitoring, January 8, 2008.
- 59 See: US Department of Homeland Security, Cybersecurity Strategy 2018, <https://publicintelligence.net/dhs-cybersecurity-strategy-2018/> (accessed August 10, 2020); See also: For an analysis of the unique challenges facing the military and the Department of Defense, review: US Department of Defense, Cybersecurity Discipline Implementation Plan February 2016, <https://publicintelligence.net/dod-cybersecurity-discipline/> (accessed August 10, 2020).
- 60 US Department of Homeland Security, Directorate of Science & Technology, Cyber Risk Economics page, <https://www.dhs.gov/science-and-technology/cyrie> (accessed August 10, 2020).
- 61 The National Threat Center, Counterintelligence Guide: The National Security Threat List, http://www.wrc.noaa.gov/wrso/security_guide/nsstl.htm (accessed August 10, 2020).
- 62 US Department of Homeland Security, National Protection and Programs Directorate, Cybersecurity Risks Posed by Unmanned Aircraft Systems, May 22, 2018, <https://info.publicintelligence.net/OCIA-UnmannedAircraftRisks.pdf> (accessed August 10, 2020).
- 63 Ibid., at 2.
- 64 Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, DC: May 2005), <http://www.gao.gov/htext/d05434.html> (accessed August 10, 2020).
- 65 US-CERT Website, Federal Incident Reporting Guidelines, at Federal Agency Incident Categories, <https://www.us-cert.gov/government-users/reporting-requirements> (accessed August 10, 2020).
- 66 Office of the President, The National Strategy to Secure Cyberspace (February 2003), x, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed August 10, 2020).
- 67 See Carnegie Mellon University, Computer Emergency Readiness Team: Vulnerability Statistics, <https://www.cert.org/vulnerability-analysis/publications/index.cfm> (accessed August 10, 2020); See also President, Strategy to Secure Cyberspace, 10.
- 68 See: US Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC) Capabilities Guide, (2013), <https://publicintelligence.net/nccic-capabilities-guide/> (accessed August 10, 2020).
- 69 Microsoft Security Intelligence Report, The Evolution of Malware and the Threat Landscape—A 10-Year Review, 20 (February 2012), <https://www.microsoft.com/en-us/download/details.aspx?id=29046/> (accessed August 10, 2020).
- 70 See: The Heritage Foundation, A Sampling of Election Fraud Cases from Across the Country, https://www.heritage.org/sites/default/files/voterfraud_download/VoterFraudCases_5.pdf (accessed August 10, 2020).
- 71 Office of the President, Homeland Security Presidential Directive 7, December 2003, 3.
- 72 President, Strategy to Secure Cyberspace, viii.
- 73 R. Skinner, Einstein presents big challenge to US-CERT. IG: US-CERT fails to adequately share critical data with agencies. GovInfo Security, June 22, 2010, www.govinfosecurity.com/p_print.php?t=a&id=2677 (accessed August 10, 2020).
- 74 Ibid., at 2.
- 75 Office of the Inspector General, Department of Homeland Security, DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems 2, July 30, 2010.
- 76 Office of the Inspector General, Department of Homeland Security, DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems 5, July 30, 2010; US-CERT Federal Incident Notification Guidelines, <https://www.us-cert.gov/incident-notification-guidelines> (accessed August 10, 2020); U.S. Dept. of Homeland Security, Office of Inspector General, Implementation Status of the Enhanced Cybersecurity Services Program, OIG-14-119 (July 2014), https://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-119_Jul14.pdf (accessed August 10, 2020).

Homeland Security

- 77 See J. G. Schwitz, Risk-based cybersecurity policy, *American Intel Journal*, 29 (2011):115.
- 78 This approach has been repeatedly advanced by those arguing for private policing systems working side by side with public policing systems. See J. F. Pastor, Public-private policing arrangements & recommendations, *The Homeland Security Review*, 4 (2010): 71; See also C. P. Nemeth and K. C. Poulin, *The Prevention Agency*, (California, PA: California University of PA Press-Institute for Law & Public Policy, 2006); C. P. Nemeth and K. C. Poulin, *Private Security and Public Safety: A Community Based Approach*, (London: Pearson, 2005); J. F. Pastor, *Terrorism and Public Safety Policing: Implications for the Obama Presidency*, (London: Routledge, 2010).
- 79 N. Santella and L. J. Steinberg, Accidental releases of hazardous materials and relevance, *Journal of Homeland Security and Emergency Management*, 8 (2011): article 53, at: <http://www.bepress.com/jhsem/vol8/iss1/53>.
- 80 Santella and Steinberg, at 11.
- 81 M. Kano et al., Terrorism preparedness and exposure reduction since 9/11: The status of public readiness in the United States, *Journal of Homeland Security & Emergency Management*, 8 (2011): 1–17.
- 82 J. Fleischman, Engaging the private sector in local homeland defense: The Orange County private sector terrorism response group, *Sheriff* (September/October, 2004): 33.
- 83 National Infrastructure Advisory Council, Public-private sector intelligence coordination: Final report and recommendations by the council, July 2006, 67.
- 84 C. P. Nemeth, *Private Security and the Law* (London: Elsevier, 2008), 12.
- 85 Homeland Security Research Corporation, Private sector to become 2nd largest homeland security industry customer by 2011, news release, April 9, 2008.
- 86 Homeland Security Research, U.S. Private Sector Homeland Security Market, 2010–2014, <https://homelandsecurityresearch.com/wp-content/uploads/2013/10/HSRC20100614TOC.pdf> (accessed August 10, 2020).
- 87 For an examination of how these privatized practices prompt ethical concerns, see K. Carmola, *Private Security Contractors in the Age of New Wars: Risk, Law & Ethics* (New York: Routledge Press, 2008).
- 88 P. Starr, The meaning of privatization, *Yale Law and Policy Review*, 6 (1988): 6–41. This article also appears in Alfred K. and S. Kamerman, eds., *Privatization and the Welfare State* (Princeton, NJ: Princeton University Press, 1989).
- 89 F. Chen, Structuring public-private partnerships: Implications from the ‘Public-Private Investment Program for Legacy Securities,’ *Columbia Journal of Law and Social Problems* 46 (2013): 509.
- 90 Private Security Officer Employment Authorization Act of 2004, U.S. Code 28, 2004, section 534.
- 91 I. P. McGinley, Regulating “rent-a-cops” post 9/11: Why the Private Security Officer Employment Act fails to address homeland security concerns, *Cardozo Public Law, Policy and Ethics*, 6 (2007): 145.
- 92 C. P. Nemeth, *Private Security and the Investigative Process*, 2nd ed. (Boston, MA: Butterworth Heinemann, 2000), 1–4.
- 93 Bureau of Justice Assistance, *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships*, 2003, 11; See also: C. P. Nemeth, *Introduction to Private Security* (2018).
- 94 National Defense Industrial Association, www.ndia.org/Aboutus/pages/default.aspx (accessed August 10, 2020).
- 95 Bureau of Justice Assistance, *Engaging the Private Sector*, 13.
- 96 See: L. Chapa, “Opening Up,” *Security Management* (February 2018), <https://www.asisonline.org/security-management-magazine/articles/2018/02/opening-up/> (accessed August 10, 2020).
- 97 B. Harrell, “The private sector is the key to success for the Department of Homeland Security,” *CSO* February 1, 2017, <https://www.csoonline.com/article/3161793/the-private-sector-is-the-key-to-success-for-the-department-of-homeland-security.html> (accessed August 10, 2020).
- 98 See: N. E. Busch and A. D. Givens. “Public-Private Partnerships in Homeland Security: Opportunities and Challenges.” *Homeland Security Affairs* 8, Article 18 (October 2012), <https://www.hsaj.org/articles/233> (accessed August 10, 2020).
- 99 See: US Department of Homeland Security, Private Sector office page, <https://www.dhs.gov/private-sector-office> (accessed August 10, 2020); See also: US Department of Homeland Security, Private Sector Resources Catalog (2012), https://www.dhs.gov/sites/default/files/publications/private_sector_resource_catalog_December_2012.pdf (accessed August 10, 2020).

- 100 See: K. Strom et al., "The Private Security Industry: A Review of the Definitions, Available Data Sources, and Paths Moving Forward," (December 2010), <https://www.ncjrs.gov/pdffiles1/bjs/grants/232781.pdf> (accessed August 10, 2020).
- 101 Ibid.
- 102 D. Ritchey, "The changing role of the CISO," *Security Magazine*, February 3, 2020, <https://www.securitymagazine.com/articles/91653-the-changing-role-of-the-ciso> (accessed August 10, 2020).
- 103 Ibid.
- 104 S. Hakim and E. A. Blackstone, The role of the private sector in homeland security. In S. Hakim and E. A. Blackstone (Eds.), *Safeguarding Homeland Security: Governors and Mayors Speak Out* (New York: Springer, 2009), 1–21; M. Clark, J. Cordes, and B. Roberts. Public-private partnerships and homeland security. *National Tax Association Proceedings*, (2006), <https://ntanet.org/wp-content/uploads/proceedings/2006/020-clark-publicprivate-partnerships-homeland-2006-nta-proceedings.pdf> (accessed August 10, 2020); National Security Council, *Sharing Information with the Private Sector*, <https://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionV.html> (accessed August 10, 2020); U.S. Department of Justice, *Engaging the private sector to promote homeland security: Law Enforcement-Private Security Partnerships*, (2005), <https://www.ncjrs.gov/pdffiles1/bja/210678.pdf> (accessed August 10, 2020).
- 105 M. Chertoff. 9/11: Before and After. *Homeland Security Affairs* 7, 10 Years After: The 9/11 Essays, (2011), <https://www.hsaj.org/articles/584> (accessed August 10, 2020); D. Ritchey. Public and private security: Bridging the gap. *Security Magazine*, June 1, 2010, <https://www.securitymagazine.com/articles/80710-public-and-private-security-bridging-the-gap-1> (accessed August 10, 2020); The White House. *Sharing information with the private sector* (n.d.), <https://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionV.html> (accessed August 10, 2020).
- 106 P. Auerswald, L. M. Branscomb, T. M. LaPorte, and E. Michel-Kerjan. The challenge of protecting critical infrastructure, *Issues in Science and Technology*, 23(1) (2005), <https://issues.org/auerswald/> (accessed August 10, 2020); D. Ritchey, "The changing role of the CISO," *Security Magazine*, February 3, 2020, <https://www.securitymagazine.com/articles/91653-the-changing-role-of-the-ciso> (accessed August 10, 2020).
- 107 U.S. DOJ. *Engaging the private sector to promote homeland security: Law Enforcement-Private Security Partnerships*, (2005), 4–6; International Association of Chiefs of Police. *National Policy Summit: Building private security/public policing partnerships to prevent and respond to terrorism and public disorder*, (2004), <https://www.theiacp.org/sites/default/files/2018-08/ACFAB5D.pdf> (accessed August 10, 2020).
- 108 D. Ritchey. Proud to be security: How roles changed after 9/11. *Security Magazine*, (September 1, 2011).
- 109 Ibid.
- 110 Ibid.
- 111 S. Hakim and E. A. Blackstone. The role of the private sector in homeland security, (2009). [see *Employing Technology*.]
- 112 Ibid.
- 113 This is why efforts at threat reduction as to nuclear arsenals are a sensible part of the homeland plan. See A. F. Woolf, *Department of Defense Cooperative Threat Reduction Program, Nonproliferation and Threat Reduction Assistance: U.S. Programs in the Former Soviet Union* (Congressional Research Service, March 6, 2012).



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

5

Training and Exercises in Homeland Security

OBJECTIVES

1. To appraise the mission of the Department of Homeland Security's (DHS) grants and training opportunities for funding
2. To describe "Top Officials" (TOPOFF), National Exercise Program (NEP), and National Level Exercise (NLE) exercises and simulation programs and identify to whom they are offered, as well as the goals of the training program
3. To explain the mission and objectives of the Center for Domestic Preparedness (CDP) and its training programs
4. To summarize the activities of the Emergency Management Institute (EMI), including their course offerings and the constituencies they serve
5. To evaluate the usefulness and effectiveness of the Homeland Security Exercise and Evaluation Program (HSEEP), the Homeland Security Digital Library (HSDL), and the Lessons Learned Information Sharing Program (LLIS.gov)
6. To compare the seven types of exercises defined by HSEEP and identify the difference between discussion-based and operations-based exercises
7. To evaluate the usefulness and effectiveness of Community Emergency Response Teams (CERTs) across the country and explain their mission and goals
8. To outline the organization, purpose, and processes of the National Incident Management System (NIMS) and its various components

5.1 Introduction

The breadth, depth, scope, and coverage of training programs in homeland security are simply mind-boggling. Not only do agencies of government at the state, local, and federal levels devise, design, and deliver training in all the affairs of homeland, but so too do a plethora of private

Homeland Security

companies and businesses. In a nutshell, training is a fast-growing business for both the public and the private sector. In the public sense, government agencies, in seeking to carry out their mission, educate the public and the professionals who must labor each day in the justice and emergency model. DHS is the preeminent figure in the training modality and delivers programs to every imaginable sector. A partial list of the agency's more prominent programs is charted in Figure 5.1.

This section will scan some of these training systems with the full recognition that it can only touch the surface of most. DHS not only delivers a wide array of educational programs but also seeds the entire country with grants and other support so that localities and nonfederal jurisdictions can educate their constituencies with a local flavor. Billions of dollars in grants flow to

FEMA Training and National Domestic Preparedness Consortium - Direct training for state and local jurisdictions to enhance capacity and preparedness

The Federal Law Enforcement Training Center - Up-to-date, low or no cost training opportunities for state and local law enforcement officers

National Preparedness Network (PREPnet) - First responder information programming schedule, all open and available to the public

The National Fire Academy - Training and educational opportunities for members of the fire, emergency services and allied professionals

Noble Training Center - Hospital-based medical training in disaster preparedness and response

The Emergency Management Institute - Training to ensure the effectiveness of organizations and individuals working together in disasters and emergencies

National Integration Center (NIC) - Incident Management Systems Division Information, guidance and resources to assist state, local, tribal and federal agencies in adopting and implementing the National Incident Management System.

National Incident Management System (NIMS) Online Training - Introduction to the purpose, principles, key components and benefits of NIMS.

Comprehensive Haz-Mat Emergency Response Capability Assessment Program (CHER-CAP) - Resource to prepare for hazardous materials incidents

National Exercise Program - Training, exercising, and collaboration among partners at all levels.

Homeland Security Exercise and Evaluation Program - Threat- and performance-based exercise activities of varying degrees of complexity and interaction

Lessons Learned Information Sharing - Best practices and lessons learned from actual terrorist events and training exercises

U.S. Fire Administration Publications - Free publications for emergency responders including manuals, reports & incident reports

Figure 5.1 DHS programs.

every state, with most major urban areas receiving additional funding—so too with various special agencies at the federal level. As this chapter makes plain, while DHS leads the overall effort in homeland security, other agencies of government have their fingers in the homeland pie. Witnessed in Chapter 11 is the oversight role of the Centers for Disease Control and Prevention (CDC) in matters of bioterrorism, chemical attacks, and other weapons of mass destruction (WMD). Other agencies, such as the Department of Agriculture, the Nuclear Regulatory Commission, the Food and Drug Administration (FDA), and the military, play integral roles as well. Both funding and training spill out to the practitioners from these agencies in the same way as DHS does.

5.2 Grants and Training

Long part of its historic mission, DHS has actively supported the training of personnel at the state, federal, and local level as well as provided direct block grants to states and localities for on-location training in various jurisdictions. DHS, since its earliest days of operation, allowed competitive grant and training processes to be available to both public and private-sector partners. During the formative stages of the department, there was a complete hodgepodge of various entities administering these activities. At present, the DHS is entwined a dizzying array of grant and training-related programs—some originating in G&T and others with a source point elsewhere in the DHS. A list of grant and training activity relevant to homeland security includes but is not limited to:

- Bioterrorism Training and Education
- Bureau of Justice Assistance National Training and Technical Assistance Center
- Center for Domestic Preparedness
- Centers for Public Health Preparedness
- Chemical Emergency Information for First Responders
- Disaster Information Specialization
- DHS Training and Exercise
- Emergency Preparedness for All Hazards
- Emergency Preparedness for Natural Disasters and Severe Weather
- Emergency Use Authorization Training
- FEMA Emergency Management Institute Course Listings
- First Responder Training
- Homeland Security Exercise and Evaluation Program
- Hydrogen Safety for First Responders
- Improvised Explosive Device Awareness Training
- International Association of Fire Fighters
- Lessons Learned Information Sharing
- Mass Casualty Event Preparedness and Response
- National Center for Forensic Scientists
- National Counterterrorism Center
- National Disaster Preparedness Training Center

Homeland Security

- National Domestic Preparedness Consortium
- National Exercise Program
- National Fire Academy Education and Training
- National Preparedness Directorate National Training and Education
- Radiological and Nuclear Terrorism Mass Casualty Training
- Ready.gov Campaign
- Suicide Prevention Resources for First Responders
- Terrorism and Preparedness Data Resource Center
- The Energetic Materials Research and Testing Center
- The National Center for Biomedical Research and Training
- The National Emergency Response and Rescue Training Center
- The U.S. Department of Energy's National Nuclear Security Administration
- Transportation Technology Center, Incorporated

DHS, in its quest for centralization and improved efficiency, blended a host of diverse offices into the Office of Grants and Training (G&T). The *Post-Katrina Emergency Reform Act of 2006* amended the Homeland Security Act and mandated some mergers and realignments. As part of this reorganization, major national preparedness components and functions, which include the Office of G&T, the United States Fire Administration, National Capital Region Coordination, Chemical Stockpile Emergency Preparedness, and the Radiological Emergency Preparedness Program, while still operational under the DHS heading, were transferred to the Federal Emergency Management Agency (FEMA), effective April 1, 2007.

The new organization reflected the expanded scope of FEMA's departmental responsibilities. It strengthens FEMA's coordination with other DHS components as well as with agencies and departments outside of DHS. It also enhances FEMA's ability to partner with emergency management, law enforcement, preparedness organizations, and the private sector. Aside from this bureaucratic realignment, the Office of G&T makes possible a bevy of training opportunities for homeland security specialists. The Directorate for Grants and Training constantly examines how the homeland security landscape evolves and changes and adjusts its grant process accordingly. The Directorate's objectives are:

- review, negotiate, award, and manage FEMA's preparedness grant portfolio;
- provide subject-matter expertise in response to regional office and stakeholder inquiries;
- develop grant guidance;
- formulate risk methodology to support grant allocations;
- analyze investments;
- manage budget execution and formulation; and
- provide the driving force for grants management initiatives through the strategic delivery of policy, training, systems, and data analysis.¹

Its mission is multifaceted but directed primarily at those in the first-responder category, such as fire and emergency medical technicians (EMT), police, and paramedics. The agency posts a well-defined mission:

5.2 Grants and Training

The mission of G&T is to prepare America for acts of domestic terrorism by developing and implementing a national program to enhance the capacity of state and local agencies to respond to incidents of terrorism, particularly those involving chemical, biological, radiological, nuclear and explosive (CBRNE) incidents, through coordinated training, equipment acquisition, technical assistance, and support for Federal, state, and local exercises.²

Soon after these mergers, FEMA set out specific strategic goals that advance its grand vision to be the “Nation’s Preeminent Emergency Management and Preparedness Agency.”³ The extensive grant programs had to be aligned with FEMA’s overall strategic goals and mission. Review Figure 5.2⁴ to see how it envisioned the compatibility of these goals as it carried out the mission.

GPD strategic goals	FEMA strategic goals				
	Goal 1: Lead an integrated approach that strengthens the nation's ability to address disasters, emergencies, and terrorist events	Goal 2: Deliver easily accessible and coordinated assistance for all programs	Goal 3: Provide reliable information at the right time for all users	Goal 4: FEMA invests in people and people invest in FEMA to insure mission success	Goal 5: Build public trust and confidence through performance and stewardship
Goal 1: Emphasize employee development and human capital planning				✓	
Goal 2: Team with internal and external stakeholders	✓		✓		
Goal 3: Provide accurate and timely information and services		✓	✓		
Goal 4: Build a robust and standardized data analysis capability	✓		✓		✓
Goal 5: Streamline, standardize and document key processes		✓			✓

Figure 5.2 Grant Programs Directorates (GPD) alignment to FEMA's strategic goals.

Homeland Security

In addition, the G&T program targets specified settings such as ports, public transport, and other critical infrastructure. The grant program encompasses all sorts of coverage:

- NEHRP Grant Program
- Procurement Disaster Assistance Team
- Emergency Management Performance Grant Program
- Homeland Security Grant Program
- Intercity Bus Security Grant Program
- Intercity Passenger Rail Security Grant Program
- Nonprofit Security Grant Program
- Port Security Grant Program
- Transit Security Grant Program
- Tribal Homeland Security Grant Program
- Presidential Residence Protection Assistance Grant
- Assistance to Firefighters Grant Program⁵

FEMA sees the entire picture of G&T in an agency–individual employee horizon, making a noble effort to connect the larger purposes of the agency’s purpose with the roles, tasks, and functions of its employees downstream. It labels this a *cascade up* or a *cascade down*. Hence, the agency authors grant and training policies that complement individual performance and the efficacy of the agency itself (see Figure 5.3).⁶

G&T fulfills this mission through a series of program efforts responsive to the specific requirements of state and local agencies. G&T works directly with emergency responders and conducts assessments of state and local needs and capabilities to guide the development and execution of these programs. Assistance provided by G&T is directed at a broad spectrum of state and local emergency responders, including firefighters, emergency medical services (EMS), emergency management agencies, law enforcement, and public officials.

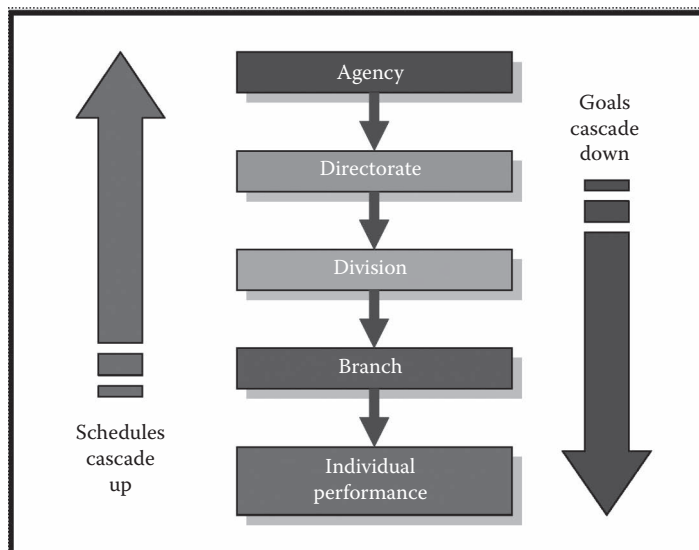


Figure 5.3 Strategy implementation chart.

5.2 Grants and Training

G&T attends to this mission in a variety of ways by providing grants to states and local jurisdictions, providing hands-on training through a number of residential training facilities and in-service training at the local level, funding and working with state and local jurisdictions to plan and execute exercises, and providing technical assistance on-site to state and local jurisdictions. In many respects, the office fervently addresses Homeland Security Presidential Directive 8, which encourages all agencies of government to be prepared, trains their personnel, and establishes a national program and a multiyear planning system to conduct homeland security preparedness--related exercises that reinforce identified training standards, provide for evaluation of readiness, and support the national preparedness goal. The establishment and maintenance of the program will be conducted in maximum collaboration with state and local governments and appropriate private sector entities.⁷ For the 2011 grant cycle, the Office of G&T prioritizes the funding of the following programs:

- State Homeland Security Program (SHSP)
- Urban Areas Security Initiative (UASI)
- Tribal Homeland Security Grant Program (THSGP)
- Nonprofit Security Grant Program (NSGP)
- Regional Catastrophic Preparedness Grant Program (RCPSP)
- Emergency Operations Center Grant Program (EOC)
- Driver's License Security Grant Program (DLSGP)
- Transit Security Grant Program (TSGP)
- Freight Rail Security Grant Program (FRSGP)
- Intercity Passenger Rail (IPR-Amtrack) Program
- Intercity Bus Security Grant Program (IBSGP)
- Port Security Grant Program (PSGP)
- Emergency Management Performance Grants (EMPG)⁸

The Office of G&T supports cooperative partnerships among all relevant homeland constituencies. By and through the National Domestic Preparedness Consortium, the Office of G&T identifies, develops, tests, and delivers training to state and local emergency responders (see Figure 5.4).

The Office of G&T has also funded equipment purchases for justice and emergency agencies. An approved equipment list is published by the department. The office has supported the following equipment acquisitions:



Figure 5.4 National Domestic Preparedness Consortium logo.

Homeland Security

- Personal protective equipment
- Equipment—explosive device mitigation and remediation
- CBRNE operational and search and rescue equipment
- Information technology equipment
- Cybersecurity enhancement equipment
- Interoperable communications equipment
- Detection equipment
- Decontamination equipment
- Medical equipment
- Power equipment
- CBRNE reference materials
- CBRNE incident response vehicles
- Terrorism incident prevention equipment
- Physical security enhancement equipment
- Inspection and screening systems
- Agricultural terrorism prevention, response, and mitigation equipment
- CBRNE prevention and response watercraft
- CBRNE aviation equipment
- CBRNE logistical support equipment
- Intervention equipment
- Other authorized equipment

The Office of G&T coordinated TOPOFF exercises and simulation programs. TOPOFF signifies “top officials” or those higher up in the homeland supervisory chain. Officials from state, local, and federal agencies work collaboratively on a homeland problem, assess and evaluate the homeland dilemma, and publish best practices in dealing with the security question. As of 2011, the Office of G&T had conducted four major TOPOFF exercises, as illustrated in Figure 5.5.

The TOPOFF program has been replaced by what is now designated the *National Exercise Program* (NEP). The NEP allows federal, state, and local agencies to work collaboratively on all sorts of risks and hazards. Thus far, there has been a variety of NEPs whose coverage has included

- *National Level Exercise 2020*: NLE 20 was postponed due to the COVID-19. Its content stressed cybersecurity
- *National Level Exercise 2018*: NLE 18 focused on emergency preparedness during hurricane. See Figure 5.6.⁹
- *National Level Exercise 2012 (NLE 12)*: NLE 12 was a series of exercise events that examined the ability of the United States to execute a coordinated response to a series of significant cyber incidents. As a part of the NEP, NLE 12 emphasized the shared responsibility among all levels of government, the private sector, and the international community to secure cyber networks and coordinate response and recovery actions.

TOPOFF 4: Increasing Coordination through Collaboration

Conducted in October 2007, TOPOFF 4 took place in Portland, Ore.; Phoenix, Ariz.; and for the first time, the U.S. territory of Guam as well as in Washington, D.C. for federal partners.

The exercise built on past lessons learned while adding new goals, including: an increased level of coordination with U.S. Department of Defense exercises to combat global terrorism, closer cooperation with the private sector, an expanded emphasis on prevention, a deeper focus on mass decontamination and long-term recovery and remediation issues, and strengthened coordination and communications with international allies.

More than 15,000 participants representing federal, state, territorial, and local entities, as well as the governments of Australia, Canada, and the United Kingdom, participated in the exercise.

All venues responded to a radiological RDD attack.

TOPOFF 3: Exercising National Preparedness

Conducted in April 2005, TOPOFF 3 was the first test of the National Response Plan (NRP) and National Incident Management System (NIMS).

TOPOFF 3 continued to evolve and included an increased focus on bolstering international and private sector participation, terrorism prevention activities, risk communication and public information functions, and long-term recovery and remediation issues.

Over 10,000 participants, including responders and officials from Canada and the United Kingdom, responded to a simulated chemical attack in New London, Conn., and a biological attack in the state of New Jersey.

The exercise marked the launch of a new simulated media tool – the interactive web site VNN.com.

TOPOFF 2: Assessing Homeland Security Planning

Conducted in May 2003, TOPOFF 2 was the first national exercise following the September 11, 2001 attacks and was led by the newly-formed Department of Homeland Security (DHS).

TOPOFF 2 provided the first opportunity for DHS to exercise its organizational functions and assets, including tests of the Homeland Security Advisory System (HSAS).

Participants in Seattle faced a simulated radiological dispersal device (RDD) attack, while those in the Chicago faced a biological attack.

The exercise engaged 8,500 responders and top officials from the United States and Canada – the first international partner to participate.

TOPOFF 2000: Coordinated, Strategic National Response

In May 2000, the Department of Justice, the Department of State, and the Federal Emergency Management Agency (FEMA) led the first exercise in the TOPOFF series.

The primary goal of the exercise was to improve the capability of government officials and agencies, both within the United States and abroad to provide an effective, coordinated, and strategic response to a terrorist attack.

More than 6,500 federal, state, and local personnel – including top officials – responded to a simulated biological attack in Denver, Colorado and a simulated chemical attack in Portsmouth, N.H.

The exercise introduced a new element in preparedness exercises: a simulated media outlet known as the Virtual News Network (VNN). VNN kept players up-to-date on unfolding events and forced decision-makers to face the challenge of communicating with real-world media in a crisis.

Figure 5.5 TOPOFF exercises through 2011.

NATIONAL LEVEL EXERCISE 2018

FEMA leads national level exercises every two years to make sure the country is prepared for disasters. In 2018, the National Level Exercise (NLE) centered on a major mid-Atlantic hurricane.

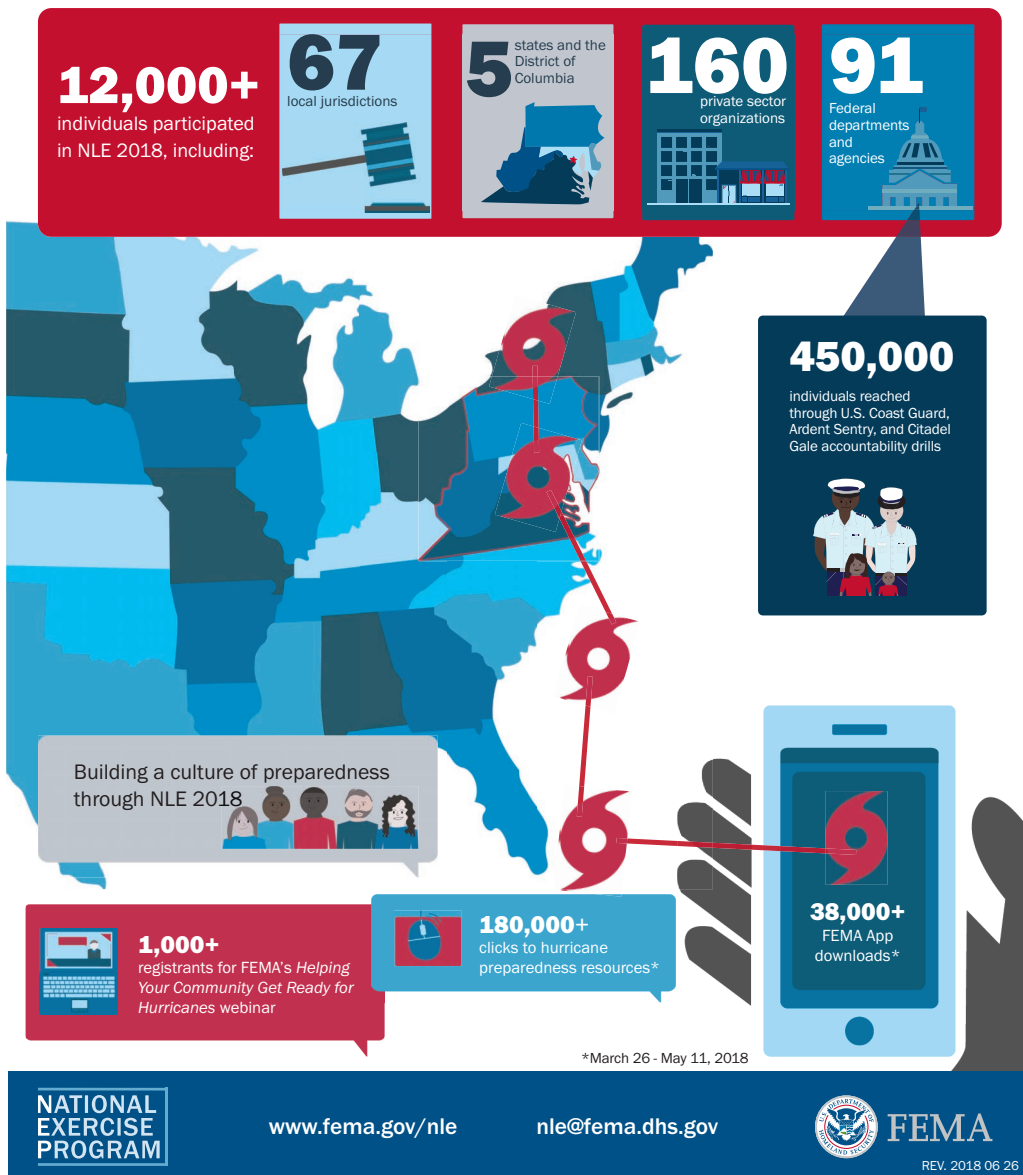


Figure 5.6 The 2018 FEMA National Level Exercise (NLE) centered on a major mid-Atlantic hurricane.

The NLE 12 series was focused on examining four major themes: planning and implementation of the draft National Cyber Incident Response Plan (NCIRP), coordination among governmental entities, information sharing, and decision-making.

- *National Level Exercise 2011 (NLE 11)*: NLE 11 was an operations-based exercise centered on the scenario of a catastrophic earthquake in the New Madrid Seismic Zone,

encompassing four FEMA regions (IV, V, VI, and VII) and eight Central U.S. earthquake states: Alabama, Arkansas, Kentucky, Illinois, Indiana, Mississippi, Missouri, and Tennessee. NLE 11 exercised initial incident response and recovery capabilities and tested and validated existing plans, policies, and procedures to include the New Madrid Catastrophic Plan.

- *National Level Exercise 2010 (NLE 10)*: FEMA conducted NLE 10 on May 17–18, 2010. NLE 10 engaged federal, state, and local partners in a series of events and opportunities to demonstrate and assess federal emergency preparedness capabilities pertaining to a simulated terrorist attack scenario involving an improvised nuclear device.
- *National Level Exercise 2009 (NLE 09)*: NLE 09 was designated as a Tier I NLE. Tier I exercises (formerly known as the Top Officials exercise series or TOPOFF) are conducted annually in accordance with the NEP, which serves as the nation's overarching exercise program for planning, organizing, conducting, and evaluating NLEs.

The NEP was established to provide the U.S. government, at all levels, with exercise opportunities to prepare for catastrophic crises ranging from terrorism to natural disasters.¹⁰

The office reserved a portion of its grant funding exclusively for firefighters and fire administration. DHS is well aware of this pressing need since so much of what fire personnel undertake often relates to hazardous activities. Three types of grants are available: Assistance to Firefighters Grant (AFG), Fire Prevention and Safety (FP&S), and Staffing for Adequate Fire and Emergency Response (SAFER) (Figure 5.7).

Eligible applicants for AFG are limited to fire departments and nonaffiliated EMS organizations operating in any of the 50 states plus the District of Columbia, the Commonwealth of the Northern Mariana Islands, the Virgin Islands, Guam, American Samoa, and Puerto Rico.¹¹

Internet Exercise: Review the various grants available through the AFG Program at <https://www.fema.gov/welcome-assistance-firefighters-grant-program>.

Without much fanfare, the Office of G&T was submerged into a host of other DHS offices and bureaucracies after the 2011 cycle. For various reasons, both political and economic, G&T was replaced by the DHS Preparedness Grant Program and the DHS Homeland Security Grant Program. Under this new umbrella, DHS continues to administer and fund a wide assortment of worthy endeavors and to train a myriad of partners and players in the world of homeland security. For the 2015 cycle of awards, DHS announced the following program initiatives:

- *Homeland Security Grant Program (HSGP)*: Provides more than \$1 billion for states and urban areas to prevent, protect against, mitigate, respond to, and recover from acts of terrorism and other threats



Figure 5.7 Assistance to Firefighters Grant Program logo.

Homeland Security

- *State Homeland Security Program (SHSP)*: Provides \$402 million to support the implementation of the National Preparedness System to build and strengthen preparedness capabilities at all levels
- *Urban Areas Security Initiative (UASI)*: Provides \$587 million to enhance regional preparedness and capabilities in 28 high-threat, high-density areas
- *Operation Stonegarden (OPSG)*: Provides \$55 million to enhance cooperation and coordination among local, tribal, territorial, state, and federal law enforcement agencies to jointly enhance security along the United States land and water borders where there are ongoing U.S. Customs and Border Protection missions
- *Emergency Management Performance Grant (EMPG) Program*: Provides over \$350 million to assist local, tribal, territorial, and state governments in enhancing and sustaining all-hazards emergency management capabilities
- *Tribal Homeland Security Grant Program (THSGP)*: Provides \$10 million to eligible tribal nations to implement preparedness initiatives to help strengthen the nation against risks associated with potential terrorist attacks and other hazards
- *Nonprofit Security Grant Program (NSGP)*: Provides \$13 million to support target hardening and other physical security enhancements for nonprofit organizations that are at high risk of a terrorist attack and are located within one of the 28 fiscal year (FY) 2015 UASI-eligible urban areas
- *Intercity Passenger Rail—Amtrak (IPR) Program*: Provides \$10 million to protect critical surface transportation infrastructure and the traveling public from acts of terrorism and increase the resilience of the Amtrak rail system
- *Port Security Grant Program (PSGP)*: Provides \$100 million to help protect critical port infrastructure from terrorism, enhance maritime domain awareness, improve port-wide maritime security risk management, and maintain or reestablish maritime security mitigation protocols that support port recovery and resiliency capabilities
- *Transit Security Grant Program (TSGP)*: Provides \$87 million to owners and operators of transit systems to protect critical surface transportation and the traveling public from acts of terrorism and to increase the resilience of transit infrastructure
- *Intercity Bus Security Grant Program (IBSGP)*: Provides \$3 million to assist operators of fixed-route intercity and charter bus services within high-threat urban areas to protect bus systems and the traveling public from acts of terrorism, major disasters, and other emergencies

Internet Exercise: Review the various grants available and the process for applying at the Homeland Security Grant Program website at <https://www.fema.gov/grants/preparedness/homeland-security>.

5.3 Center for Domestic Preparedness

The CDP operates within the FEMA construct and delivers key training and education in specialized fields. Located in Aniston, Alabama, the CDP is fully accredited and is a comprehensive facility that provides resident, commuter, and online training in highly technical areas. Its specialty training relates to WMD. At the Chemical, Ordnance, Biological, and Radiological Training Facility (COBRATF), the CDP offers the only program in the nation featuring civilian training exercises in a true toxic environment, using chemical agents. The array of subject matter expertise is quite extensive. See Figure 5.8.¹²

5.4 Emergency Management Institute

The screenshot displays the FEMA Center for Domestic Preparedness website. The header includes the FEMA logo, the text "Center for Domestic Preparedness", and navigation links: Home, Contact, Continuing Education, About, News, Find Training, Apply for Training, VILT, Online Training, and Prepare for Training. A "Log in" link is also present.

The main content area is divided into two columns. The left column, titled "Select your discipline to find relevant courses", features a grid of 16 icons representing different disciplines: Law Enforcement, Fire Service, Healthcare, Emergency Medical Services, Emergency Management, Public Health, Governmental Administrative, Hazardous Materials, Public Safety Communications, Security and Safety, Education, Information Technology, Citizen/Community Volunteer, Transportation, Search and Rescue, Agricultural Safety, and Public Works.

The right column, titled "Know what you're looking for?", contains a search bar with the placeholder text "type a keyword or course name to find a course...". Below the search bar are four buttons: "View a schedule of upcoming training", "View all courses", "View all Integrated Capstone Events (ICE)", and "View Online Training". A fifth button, "View Virtual Classroom and Webinar Opportunities", is located below the "View Online Training" button.

Below these buttons is a section titled "Do you have a promo code?". It includes a text box for entering a promo code and an "Apply" button. The text below the text box states: "Enter a promo code to begin the registration process. You will be taken to a new page to further complete your application."

Below the promo code section is a section titled "Looking for training close to you?". It includes a text box for entering a zip code and a "Find Training" button. The text below the text box states: "See classes available in your area and find out more information about them."

At the bottom of the right column is a section titled "Training Information". It lists various training options: Resident training, Non-Resident Training, Indirect Training, Federal Employee Training, Private Sector, Accreditation, and Training Partners.

The footer of the website includes the FEMA logo, the text "Center for Domestic Preparedness", and contact information: 51 Responder Dr., Emmitsburg, MD, 21723, 1-866-213-9353 between the hours of 7:00 a.m. and 4:00 p.m. CST. It also includes a link to "Find additional contact information" and social media icons for Facebook, Twitter, YouTube, and LinkedIn.

Figure 5.8 The FEMA Center for Domestic Preparedness website.

The advanced, hands-on training enables responders to effectively respond to real-world incidents involving chemical, biological, explosive, radiological, or other hazardous materials.

Internet Exercise: Visit the CDP Training Portal for Educational Program Offerings at <https://cdp.dhs.gov/find-training>.

The CDP educates homeland professionals with graduated levels of sophistication and recognizes the most highly proficient practitioners. FEMA's CDP has trained more than 1.1 million local, state, and tribal responders from across the United States in preventing and responding to disasters and other terrorist threats involving CBRNE materials.¹³

Internet Exercise: See a video overview of the CDP at <https://www.youtube.com/watch?v=Hep6E2ih-sw&feature=youtu.be>

5.4 Emergency Management Institute

EMI, located in Emmitsburg, Maryland, is the lead national emergency management training, exercising, and education institution. EMI is located on a pristine campus near



Figure 5.9 EMI in Emmittsburg, MD.

Mt. St. Mary's College and shares its facilities with the U.S. Fire Administration's training center (see Figure 5.9).

EMI offers a plethora of course offerings covering all aspects of emergency preparedness in conjunction with its agency partners. The scope and influence of EMI have been significant since it has served an impressive number of customers:

In 2018, EMI offered 499 courses to support the emergency management community which were both on campus at EMI or field based. In addition, there were 193 Independent Study courses designed for online distance learning.¹⁴

A partial listing of course offerings includes:

- *E0101: Foundations of Emergency Management*
- *E0102: Science for Disasters*
- *E0103: Planning*
- *E0104: Exercise Design*
- *E0105: Public Information and Warning*
- *E0110: Foundations of Emergency Management Train-the-Trainer*
- *E0122: Emergency Management Accreditation Program (EMAP) Training Course*
- *E0133: Operations-Based Exercise Design and Evaluation (MEPP Candidates only)*
- *E0141: Instructional Presentation and Evaluation Skills*
- *E0157: Hazard Mitigation Community Education and Outreach (CEO) Specialist Qualifying Course*
- *E0158: Hazard Mitigation Community Planner Specialist Qualifying Course*
- *E0167: Core Principles for HM HPA Specialists*
- *E0180: Core Principles for Hazard Mitigation Insurance Specialists*
- *E0197: Integrating Access and Functional Needs into Emergency Planning*
- *E0202: Debris Management Planning for State, Tribal, and Local Officials*

5.4 Emergency Management Institute

- *E0207*: Introduction to Hazard Mitigation Field Operations
- *E0272*: Managing the Floodplain Post-Disaster
- *E0273*: Managing Floodplain Development through the NFIP
- *E0274*: National Dam Safety Program Technical Seminar (NDSPTS)
- *E0285*: Providing Post-Disaster Substantial Damage Technical Assistance to Communities
- *E0291*: Community Dam Safety, Preparedness, and Mitigation
- *E0296*: Application of Hazus-MH for Risk Assessment
- *E0313*: Basic Hazus-MH
- *E0337*: Posting IFMIS Transactions
- *E0349*: Mission Assignment (MA) Processing
- *E0352*: Crisis Counseling Assistance and Training Program: Training State Trainers
- *E0361*: Multi-Hazard Emergency Planning for Schools
- *E0364*: Multihazard Emergency Planning for Schools
- *E0426*: Implementing Whole Community Resilience and Citizen Corps Programs
- *E0542*: Basic Mediation Skills
- *E0580*: Emergency Management Framework for Tribal Governments
- *E0604*: Emergency Manager Orientation (EMO)/FEMA Incident Workforce Academy (FIWA) Tier IV-Specialist
- *E0706*: Disaster Contracting
- *E0726*: Financial Management Concepts for Disaster Operations
- *E0791*: Interagency Consultation for Endangered Species
- *E0827*: Geospatial Information System Managers and Unit Leaders
- *E0953*: NIMS ICS All-Hazards Public Information Officer TTT
- *E0955*: NIMS ICS All-Hazards Safety Officer TTT
- *E0968*: NIMS ICS All-Hazards Logistics Section Chief TTT

Internet Exercise: For a complete listing of the current FEMA courses, visit listing and catalog at <https://training.fema.gov/emcourses/emicalog.aspx>

EMI supports national and international emergency management with more than 50 countries participating in EMI's training and educational activities. EMI also enjoys close relations with several nationally recognized professional emergency management and related organizations, such as the International Association of Emergency Managers (IAEM), the National Emergency Management Association (NEMA), the Association of State Flood Plain Managers (ASFPM), the American Public Works Association (APWA), the American Society of Civil Engineers (ASCE), and the American Society of Engineering Management (ASEM). EMI is fully accredited by the International Association for Continuing Education and Training (IACET) and the American Council on Education (ACE). In the last decade, EMI has delivered hundreds of residential courses at the National Emergency Training Center (NETC) campus, training nearly 20,000 individual students. The EMI IS Program, a web-based distance learning program open to the public, has delivered extensive online training in 62 courses and has trained more than 2.8 million individuals. The EMI IS website receives from 2.5 to 3 million visitors a day.

Homeland Security

EMI operates the Disaster Field Training Operations (DFTO) Program. The mission of the DFTO is to “Plan, develop, promote and deliver disaster performance improvement and training opportunities in coordination with the Emergency Management Institute and Regional Offices. The Disaster Field Training Operations provides training to the Federal disaster workforce in support of FEMA’s mission.”¹⁵ In 2010 alone, the DFTO trained 31,834 disaster response and recovery employees at disaster sites throughout the United States¹⁶ (Figure 5.10).

EMI conducts national-level conferences that are well received, including the National Preparedness Annual Training and Exercise Conference and the EMI Higher Education Conference. The conference collects and catalogs institutions, course materials such as syllabi and university texts, and programmatic directions in emergency management. EMI has just implemented a School Program,¹⁷ which prepares elementary and secondary administrators for risk and threat.

Internet Exercise: See the EMI compilation of college and university syllabi at <https://www.training.fema.gov/hiedu/syllabi.aspx/>.

There are 16 critical infrastructure and key resources designated by DHS and Presidential Policy Directive/PPD-21:¹⁸

- Chemical sector
- Commercial facilities sector
- Communications sector
- Critical manufacturing sector
- Dams sector
- Defense industrial base sector
- Emergency services sector
- Energy sector
- Financial services sector
- Food and agriculture sector
- Government facilities sector
- Healthcare and public health sector
- Information technology sector



Figure 5.10 Firefighters in training at EMI.

5.5 Homeland Security Exercise and Evaluation Program

- Nuclear reactors, materials, and waste sector
- Transportation systems sector
- Water and wastewater systems sector

5.5 Homeland Security Exercise and Evaluation Program

The HSEEP, a unit of DHS, provides a standardized methodology and terminology for exercise design, development, conduct, evaluation, and improvement planning. HSEEP develops national standards for training exercises and promulgates means and modalities of assessments and evaluation to ensure agency efficiency.¹⁹ The key component of HSEEP is the design and implementation of exercises—simulations and reenactments of events and circumstances likely to be encountered in the world of homeland security. Exercises allow homeland security and emergency management personnel, from first responders to senior officials, to train and practice prevention, protection, response, and recovery capabilities in a realistic but risk-free environment. See Figure 5.11.²⁰

The intent of HSEEP is to provide a common exercise policy and program guidance capable of constituting a national standard for all exercises. HSEEP employs consistent terminology and protocols that can be used by agencies and individuals universally. HSEEP traditionally published its recommendations in a series of volumes, all of which were consolidated in 2013. The protocol and doctrine of HSEEP are summarized in chapter format:

- *Chapter 1: HSEEP Fundamentals* describes the basic principles and methodology of HSEEP.
- *Chapter 2: Exercise Program Management* provides guidance for conducting a Training and Exercise Planning Workshop (TEPW) and developing a multiyear Training and Exercise Plan (TEP).
- *Chapter 3: Exercise Design and Development* describes the methodology for developing exercise objectives; conducting planning meetings; developing exercise documentation; and planning for exercise logistics, control, and evaluation.
- *Chapter 4: Exercise Conduct* provides guidance on setup, exercise play, and wrap-up activities.
- *Chapter 5: Evaluation* provides the approach to exercise evaluation planning and conduct through data collection, analysis, and development of an after-action report (AAR).
- *Chapter 6: Improvement Planning (IP)* addresses corrective actions identified in the exercise IP and the process of tracking corrective actions to resolution.²¹

HSEEP advises agencies on best practices and lessons learned in given scenarios. All training conducted under the HSEEP banner adheres to the training template charted in Figure 5.12.²²

For the exercise to be educationally meaningful and realistically based, the following criteria need to be considered in the development process from concept to implementation:

- Setting the exercise foundation by reviewing elected and appointed officials' guidance, the TEP, and other factors
- Selecting participants for an exercise planning team and developing an exercise planning timeline with milestones
- Developing exercise-specific objectives and identifying core capabilities based on the guidance of elected and appointed officials
- Identifying evaluation requirements



FEMA

Information Sheet

Homeland Security Exercise and Evaluation Program (HSEEP) 2020 Revision

What is New in 2020

FEMA updated the Homeland Security Exercise and Evaluation Program (HSEEP) Doctrine this year with input from the whole community. The 2020 revision summarizes critical exercise information in an easier-to-reference format which will include updated templates and the HSEEP course at some point. The 2020 revision includes the following key changes:

Introduction

Whole Community: HSEEP was revised to be inclusive of the whole community to ensure better exercise outcomes by building multi-stakeholder consideration into every phase of exercise development.

Capabilities: Refers to whole community preparedness goals and not just the Core Capabilities mentioned in the National Preparedness Goal.

Senior Leaders: Involves all decision makers, not just “appointed and elected officials”.

Acronyms: Spells out all acronyms throughout the document to assist new users to adapt to exercise specific terminology.

Tools and Training: Includes references to available FEMA tools and training to make the reader aware of the entire family of support options when designing and developing an effective exercise.

Program Management

Integrated Preparedness Cycle: A continuous process of planning, organizing/equipping, training, exercising, and evaluating/improving that ensures the regular examination of ever-changing threats, hazards, and risks. Preparedness priorities are developed to ensure that the needed preparedness elements are incorporated through this continual and reliable approach to achieve whole community preparedness.

Integrated Preparedness Planning Workshop: A meeting that establishes the strategy and structure for an exercise program and preparedness efforts while setting the foundation for the planning, conduct and evaluation of individual exercises.

Integrated Preparedness Plan: A document for combining efforts across components of the Integrated Preparedness Cycle to make sure that a jurisdiction/organization has the capabilities to handle threats and hazards. The IPP allows for a more deliberate approach to multi-year preparedness activity planning.

HSEEP Fundamental Principles

The following principles frame the common approach to HSEEP:

- Guided by senior leaders;
- Informed by risk;
- Capability-based, objective-driven;
- Progressive exercise planning approach;
- Common methodology; and
- Whole Community integration.

Exercise Design and Development

Tables: Condenses the descriptions of planning meetings, exercise types, exercise documents, and tabular formats to provide easier access.

Organizational Charts: Provided to show examples of planning teams, conduct, evaluation, and exercise control structures. Removes the Incident Command System structure as a planning framework to allow for greater flexibility in whole community staffing.

Exercise Conduct

Discussion-Based and Operations-Based Exercises: Clarifies the important distinction between discussion-based vs operations-based exercises by describing each in separate sections.

Evaluation

Data Analysis: Includes a greater variety of analysis techniques to include Data Synthesis, Event Reconstruction, Trend Analysis, and Root Cause Analysis.

Improvement Planning

SMART Corrective Actions: Applies the SMART concept to post-exercise activities. SMART ensures that corrective actions are developed to be *Specific, Measurable, Achievable, Relevant, and Time-bound*.

Rev. 2020 HSEEP IS01

Figure 5.11 The 2020 Revision of the FEMA Homeland Security Exercise and Evaluation Program (HSEEP).

- Developing the exercise scenario
- Creating documentation
- Coordinating logistics
- Planning for exercise control and evaluation²³

5.5 Homeland Security Exercise and Evaluation Program



Figure 5.12 HSEEP exercise cycle.

There are seven types of exercises defined within HSEEP, each of which is either discussion-based or operations-based. Discussion-based exercises include:

- *Seminar*: A seminar is an informal discussion designed to orient participants to new or updated plans, policies, or procedures.
- *Workshop*: A workshop resembles a seminar but is employed to build specific products, such as a draft plan or policy.
- *Tabletop exercise (TTX)*: A TTX involves key personnel discussing simulated scenarios in an informal setting.
- *Games*: A game is a simulation of operations that often involves two or more teams, usually in a competitive environment, using rules, data, and procedures designed to depict an actual or assumed real-life situation.

Operations-based exercises include

- *Drill*: A drill is a coordinated, supervised activity usually employed to test a single specific operation or function within a single operation.
- *Functional exercise (FE)*: An FE examines or validates the coordination, command, and control between various multiagency coordination centers.
- *Full-Scale exercise (FSE)*: An FSE is a multiagency, multijurisdictional, multidisciplinary exercise involving functional response.

See Figure 5.13.²⁴

For operations-based exercises, HSEEP recommends broad-based participation and the widest array of agency inclusion feasible. HSEEP publishes a recommended list of participants for the planning phase of the exercise:

Emergency management

- Emergency manager
- Homeland security

Homeland Security

Full-Scale Exercise (FSE): An operations-based exercise that is typically the most complex and resource-intensive of the exercise types and often involves multiple agencies, jurisdictions/organizations, and real-time movement of resources.	
Element	Considerations and Activities
Purpose	- Often includes many players operating under cooperative systems such as the Incident Command System (ICS) Unified Command - Focus on implementing and analyzing the plans, policies, and procedures that may have been developed in discussion-based exercises and honed during previous, smaller exercises
Structure	- Events are projected through an exercise scenario with event updates that drive activity at the operational level - Involves multiple agencies, organizations, and jurisdictions - Use of a MSEL drives player actions - SimCell controllers inject scenario elements - The level of support needed may be greater than that needed for other types of exercises - Conducted in a realistic environment to mirror a real incident by presenting complex problems
Participant Goals	- Demonstrate roles and responsibilities as addressed in plans and procedures - Coordinate between multiple agencies, organizations and jurisdictions
Conduct Characteristics	- Rapid problem solving; critical thinking - Mobilization of personnel and resources - Exercise site is usually large with many activities occurring simultaneously - Site logistics require close monitoring - Safety issues, particularly regarding the use of props and special effects, must be monitored - Demonstrate roles and responsibilities as addressed in plans and procedures
Outcomes	- Validate plans, policies, and procedures - Evaluate resource requirements - An After-Action Report (AAR)/Improvement Plan (IP)

Figure 5.13 The purpose of FSE elements, considerations, and activities.

- Public health
- Public works
- Transportation/transit authority
- Public affairs
- Exercise venue/site management (e.g., stadium security)

Fire

- Fire department
- Communications/dispatch
- Special operations (e.g., hazmat, Metropolitan Medical Response System [MMRS])
- Mutual aid fire

5.5 Homeland Security Exercise and Evaluation Program

Law enforcement

- Police
- Special operations (e.g., bomb squad, Special Weapons and Tactics [SWAT])
- Sheriff's department
- Local Federal Bureau of Investigation (FBI)
- Mutual aid law enforcement

Medical

- Hospital representatives (primary trauma center or hospital association)
- Emergency medical services (i.e., public and private)
- Mutual aid
- Medical examiner/coroner

Internet Exercise: For an overview of the HSEEP process, see the PowerPoint at <https://dem.nv.gov/uploadedFiles/demnv.gov/content/raining/HSEEP%20GUIDE%20-%20Module%202.pdf>

In discussion-based exercises, the participants consider the threat and security dilemma involved and then determine the necessary players. In other words, not all homeland security threats will need medical personnel, nor will law enforcement necessarily be the preeminent actor in a homeland security dilemma.

Whatever the chosen exercise, make sure the exercise leads to achievable and measurable results in terms of understanding and performance. HSEEP publishes an excellent graphic that prioritizes the exercise's overall purpose, shown in Figure 5.14.²⁵

HSEEP urges agency trainers and instructional personnel to target the purpose and end of any selected training exercise. At a minimum, make the exercise count for something; make it relevant and meaningful for the participants and players and see the entire process as one of agency improvement. Keep the factors in Figure 5.15²⁶ in mind when developing your exercise priorities.

SMART Guidelines for Exercise Objectives		
Specific		Objectives should address the five Ws- who, what, when, where, and why. The objective specifies what needs to be done with a timeline for completion.
Measurable		Objectives should include numeric or descriptive measures that define quantity, quality, cost, etc. Their focus should be on observable actions and outcomes.
Achievable		Objectives should be within the control, influence, and resources of exercise play and participant actions.
Relevant		Objectives should be instrumental to the mission of the organization and link to its goals or strategic intent.
Time-bound		A specified and reasonable timeframe should be incorporated into all objectives.

Figure 5.14 SMART guidelines for exercise objectives.

Focus	Factors to Consider
Threats and Hazards	▪ Jurisdictional threats and hazards ▪ National threats and hazards ▪ Hazard vulnerability analysis ▪ Risk assessments
Areas for Improvement and Capabilities	▪ Real-world incident corrective actions ▪ Exercise corrective actions ▪ Identified and/or perceived areas for improvement ▪ Validating training efforts ▪ Newly acquired capabilities and resources
External Sources and Requirements	▪ Industry reports ▪ State or national preparedness reports ▪ Homeland security strategies ▪ Grants or funding-specific requirements
Accreditation Standards and Regulations	▪ Accreditation requirements ▪ Local, state, and federal regulations

Figure 5.15 Factors for consideration in developing exercise program priorities.

Professional participation makes far more sense when those enrolled understand the nature of the training, its ultimate purpose, and how the training achieves a homeland security purpose.

5.6 Lessons Learned: Best Practices (LLIS.GOV)/
Homeland Security Digital Library (HSDL)

Training, in order to be effective, must correlate to best practices and success in the field. Training that lacks the cohesion of theory and application—training that appears disconnected from a stated goal or end—lacks relevance to those laboring in homeland security. With so much at stake and so many opportunities for intellectual and practical advancement in the field, those entrusted with training must be mindful of its effectiveness. The Lessons Learned Information Sharing (LLIS) Program²⁷ promotes preparedness by identifying lessons learned and innovative practices, analyzing recurring trends, and sharing knowledge with the whole community. The web page and various requirements have just undergone a major overhaul, and the entire LLIS.GOV content library has moved and is now stored in the HSDL location. In addition, FEMA’s LLIS program consolidated their content with the Naval Postgraduate School’s HSDL who oversees the content and makes available to the public.

Internet Exercise: Visit the searchable HDSL library location which now stores all LLIS information at: <https://www.hSDL.org/?search&collection=public&fct&advanced=&submitted=Search&tabsection=LLIS+Collection>

LLIS research results deliver the practices that work, not the initiatives that simply get played and replayed due to some mindless funding or programmatic fad. These and other results from collaboration, once protected are freely shared with our homeland partners and even the public Terrorists, hoping to discern our security practices, can never be fully prevented from access to all information that homeland professionals work with and for the most part cooperation and

5.6 Lessons Learned: Best Practices (LLIS.GOV)/Homeland Security Digital Library (HSDL)

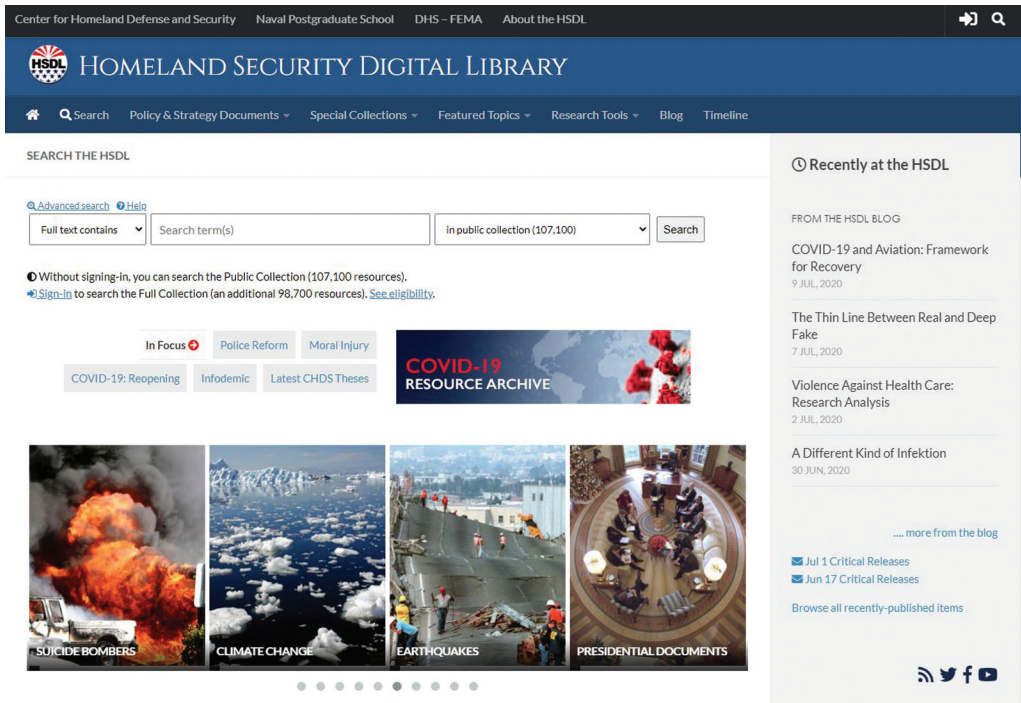


Figure 5.16 HSDL web page.

sharing work to prepare our defense front. FEMA Learned and best practices are peer-validated homeland security professionals. AARs and an information clearinghouse are cataloged and monitored and include the bulk of serious and significant documents for homeland security. A good example of this collaboration is the SAFECOM program.²⁸

Other LLIS research contained in the HDSL includes but is not limited to:

- *Lessons learned* are positive or negative experiences derived from actual incidents, operations, training, or exercises.
- *Best practices* are peer-validated techniques, procedures, and solutions that have demonstrated their effectiveness in operations, training, and exercises across multiple jurisdictions or organizations.
- *Practice notes* describe procedures, techniques, or methods that have been adopted by a single jurisdiction or organization.
- *Good stories* describe successful, innovative programs, and initiatives developed by a jurisdiction that others may wish to emulate.

The HSDL is housed and maintained by the Naval Postgraduate School in California serving as repository for all LLIS, AAR's as well as an updated list of homeland security documents from DHS and other federal, state, and local organizations, validated by subject matter experts.²⁹ See Figure 5.16³⁰

The digital library has done a superlative job of making COVID-19 resources available to a host of constituencies and has become a rich center for information regarding the many challenges posed by this pandemic. See Figure 5.17.³¹

Internet Exercise: Visit the Naval Postgraduate School website at: <https://nps.edu/>

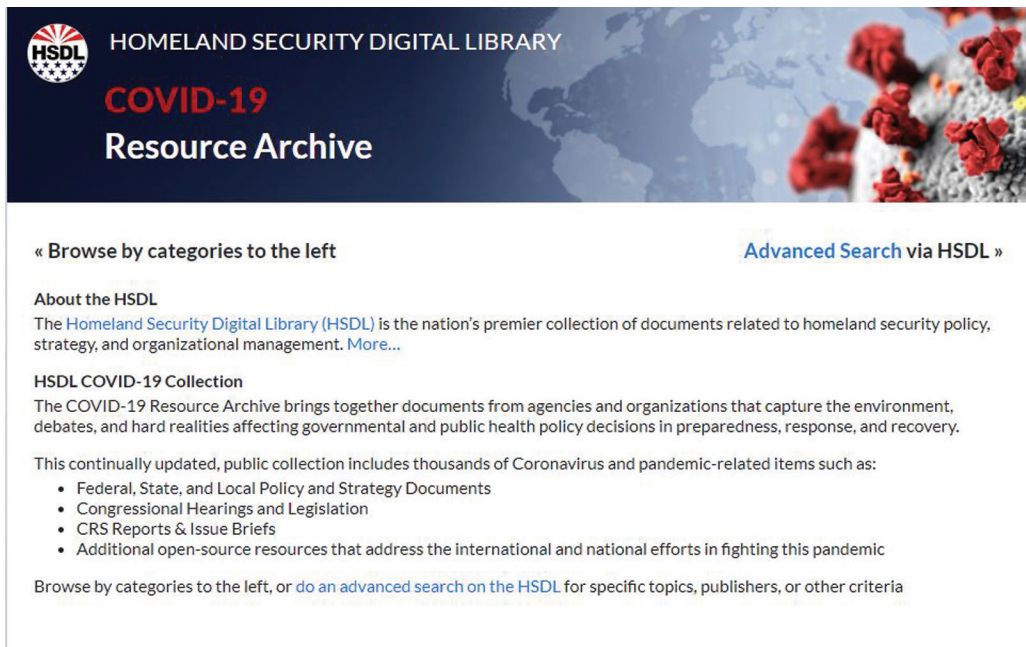


Figure 5.17 The Homeland Security Digital Library.

5.7 Community Emergency Response Teams

Another avenue of education and training rests with CERT training and CERT teams. The CERT Program educates people about disaster preparedness, the nature of hazards, and basic disaster response skills such as fire safety, light search and rescue, team organization, and disaster medical operations. CERT teams dot the entire American landscape and serve a crucial educational function.³²

CERT personnel train to prepare for a disaster or overwhelming events by

- Identifying and mitigating potential hazards in the home and workplace
- Initiating plans to prepare themselves and their loved ones for the hazards that they face
- Learning skills to help themselves, loved ones, and neighbors or fellow employees until professional response resources arrive
- Working cooperatively as a team within their neighborhoods or workplaces
- Maintaining a relationship with the agency that sponsors the CERT program
- Participating in continuing education and training
- Volunteering for projects to enhance the public safety of their communities
- Understanding their capabilities and limitations when deployed

Internet Exercise: See the CERT tutorial on search and rescue at https://www.fema.gov/media-library-data/1446229198545-36ec1e690d9e70130fc4837f56afaf8c/section_05_unit_5_ppt_102715_508.pdf.

The array of training and educational opportunities for the general citizenry wishing to be active participants is quite impressive. Many of the programs lead to certifications and most can be done online. See Figure 5.18.³³

The Updated CERT Basic Training is Here!

The updated CERT Basic Training is here! It features a revised Disaster Medical Operations section, updated Terrorism and CERT section, and new hazard-specific annexes. Find the new curriculum materials online and [order free copies from the FEMA publications warehouse beginning January 8, 2020](#).

The CERT Basic Training includes research-validated guidance for CERT programs to teach members what to do before, during, and after the hazards their communities may face. The materials in the training include:

- instructor guides;
- participant manuals;
- hazard annex slide decks
- [FEMA Independent Study IS-317: Introduction to CERT](#) can be taken online before or during training.

CERT members in leadership positions are encouraged to take the CERT Train-the-Trainer and Program Manager Courses. Find more information through the [Emergency Management Institute \(EMI\)](#) and signup for course offerings too.

2019 CERT Basic Training Materials

Instructor Guide

- [CERT Instructor Guide - English](#)
- [CERT Instructor Guide Hazard Annex - English](#)
- [CERT Instructor Guide - Spanish](#)
- [CERT Instructor Guide Hazard Annex - Spanish](#)
- [CERT Instructor Guide - Simplified Chinese](#)
- [CERT Instructor Guide Hazard Annex - Simplified Chinese](#)

Participant Manual

- [CERT Participant Manual - English](#)
- [CERT Participant Manual Hazard Annex - English](#)
- [CERT Participant Manual - Spanish](#)
- [CERT Participant Manual Hazard Annex - Spanish](#)
- [CERT Participant Manual - Simplified Chinese](#)
- [CERT Participant Manual Hazard Annex - Simplified Chinese](#)
- [CERT Participant Manual - Korean](#)
- [CERT Participant Manual - Traditional Chinese](#)
- [CERT Participant Manual - Vietnamese](#)

Figure 5.18 The CERT basic training materials website.

Much more can be said about the critical role that training and education play in the world of homeland security. Throughout this text, there will be other references to the training mentality that is now so heavily engrained in the task of homeland security. In other portions of this text, you have already analyzed the role of the Federal Law Enforcement and Training Center (FLETC)—a place where training goes on day and night. And there are other forums in the mix, such as the U.S. Fire Administration, the National Fire Academy, and the Community

Homeland Security

Hazards Emergency Response-Capability Assurance Process (CHER-CAP). You can visit these and many locations as you discover the world of homeland security.

Internet Exercise: Visit the National Fire Academy at <http://www.usfa.dhs.gov/nfa>. Visit the U.S. Fire Administration at <http://www.usfa.dhs.gov/about>.

5.8 National Incident Management System

Another approach relevant to preparedness and readiness is the NIMS.³⁴ NIMS is a by-product of Homeland Security Presidential Directive 5, which held that

To prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies, the United States Government shall establish a single, comprehensive approach to domestic incident management. The objective of the United States Government is to ensure that all levels of government across the Nation have the capability to work efficiently and effectively together, using a national approach to domestic incident management. In these efforts, with regard to domestic incidents, the United States Government treats crisis management and consequence management as a single, integrated function, rather than as two separate functions.³⁵

FEMA takes the lead in the administration of the NIMS program. FEMA’s National Integration Center (NIC) Incident Management Systems Integration Division was established by the secretary of Homeland Security to oversee NIMS and provide a research and evaluation arm regarding its standards and procedures (see Figure 5.19).

In 2020, FEMA issued improved guidance on the many aspects of the NIMS program with special emphasis on the NIMS Training Program and its prime objectives:

- 1. Describe the national approach to NIMS training;
- 2. Define NIMS training for all incident personnel;
- 3. Provide guidance to individuals and organizations wishing to pursue advanced qualifications;
- 4. Define components of an organizational training plan;
- 5. Define roles and responsibilities at all levels to provide consistent NIMS training on a national scale.³⁶

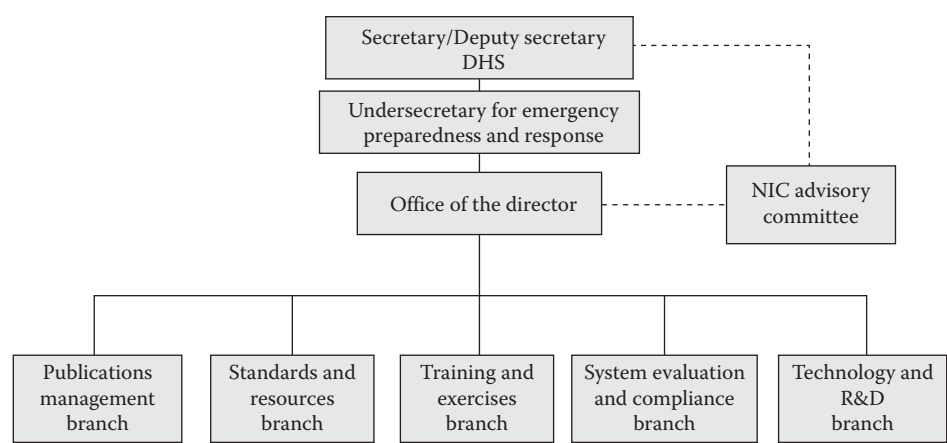


Figure 5.19 NIMS Integration Center (NIC) organization chart.

5.8 National Incident Management System

The NIMS mandate extends to every sector of government. Each and every agency of government has to plan and prepare for disaster—and must do so internally as well as externally by working efficiently and effectively with all other departments of government. While many of the NIMS functions and tasks have remained constant over the years, the NIMS program revisits its overall aim and purpose annually. In 2017, the NIMS program was “refreshed” and renewed, with special emphasis on the following areas:

- Retains key concepts and principles of the 2004 and 2008 versions of NIMS;
- Reflects and incorporates policy updates and lessons learned from exercises and real incidents;
- Clarifies the processes and terminology for qualifying, certifying, and credentialing incident personnel, building a foundation for the development of a national qualification system;
- Clarifies that NIMS is more than just the Incident Command System (ICS) and that it applies to all incident personnel, from the incident command post to the National Response Coordination Center;
- Describes common functions and terminology for staff in Emergency Operations Centers (EOC), while remaining flexible to allow for differing missions, authorities, and resources of EOCs across the nation; and
- Explains the relationship among ICS, EOCs, and senior leaders/policy groups.³⁷

NIMS reflects the clear and unbridled need for less turf protection by departments and more cooperation along federal, state, and local lines. NIMS expects that the following parties and entities will work to a common purpose regarding terror and disaster:

- Federal government
- States
- Territories
- Cities, counties, and townships
- Tribal officials
- First responders

NIMS extends to the private sector as well as to facilities of import, such as hospitals, power plants, and chemical and other related industrial centers, and all are expected to be on the same page. NIMS provides a systematic, proactive approach, guiding departments and agencies at all levels of government, in the private sector, and in nongovernmental organizations to work seamlessly to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment. This consistency mirrors the need for uniform practices in the world of homeland security and ensures predictable and dependable protocols when dealing with terror or disaster.

Internet Exercise: For a suggested NIMS plan for business and industry as to business continuity, published by FEMA, see <https://www.fema.gov/media-library/assets/documents/89510>.

The NIMS program is broken down into various components. First, compliance as to standards and practices in incident command and response is required. To accomplish this, the NIMS Compliance and Technical Assistance Branch relies on input from federal, state, local, tribal, multidiscipline, and private-sector stakeholders to ensure continuity and accuracy of ongoing implementation efforts. Compliance ensures that best practices are adopted and that ineffective programs and stratagems are abandoned. Each year, DHS issues compliance standards for both the public and the private sector.³⁸

Homeland Security

Next, the NIMS program depends on a common command and managerial structure to identify, respond to, and mitigate risk and harm. The NIMS command and management construct finds a home in the Incident Command System (ICS). ICS is a standardized on-scene incident management concept designed specifically to allow responders to adopt an integrated organizational structure equal to the complexity and demands of any single incident or multiple incidents without being hindered by jurisdictional boundaries. Before the ICS, the handling of disaster, catastrophe, or terror could only be described as nonuniform. Each incident would be tackled differently depending on the jurisdiction. The differences were starkly apparent with personnel and chain of command. Unpredictable communications systems that are incompatible and lacking interoperability caused a lack of interagency communication; and even language, often confusing and contradictory, triggers enormous challenges in the homeland community. The ICS promotes uniformity of practice, multiagency coordination, and a public information system that all constituencies can comprehend. The ICS, instead of a fractured hodgepodge of differing practices, brings to the table a common language, a common set of operating principles, and a sorely needed standardization to terror and disaster.

The ICS usually takes the form illustrated in Figure 5.20.³⁹

The ICS stresses preparedness in every context of homeland protection. Preparedness involves an integrated combination of planning, training, exercises, personnel qualification and certification standards, equipment acquisition and certification standards, and publication management processes and activities.

Planning also takes center stage in the ICS model. Plans describe how personnel, equipment, and other resources are used to support incident management and emergency response activities. Plans provide mechanisms and systems for setting priorities, integrating multiple entities and functions, and ensuring that communications and other systems are available and integrated in support of a full spectrum of incident management requirements.

Other characteristics of the ICS emphasize the importance of training for personnel—not only for internal agency preparation but also multiagency coordination. NIMS training modules are professionally developed and widely available to the professional community. NIMS participants have a bevy of opportunities for continuing education and by various means such as independent study, online or residential. With more than 290 designated courses, there is no shortfall in training for the many constituencies in homeland security. Table 5.1 provides a sample page from the educational catalog.⁴⁰

NIMS command staff author realistic training exercises in which organizations and personnel participate. Interoperability and other multiagency interactions are the key thrusts in these exercises. Drills and exercises are often used to test disaster and emergency response plans and to provide qualitative and quantitative measurements as to the effectiveness of the plan. Exercises that involve responders from multiple disciplines and multiple jurisdictions are the best way to measure the incorporation of NIMS principles and practices and provide a measurement criterion for NIMS compliance.

The ICS provides mechanisms for personnel, institutions, and equipment to be certified or officially endorsed. NIMS provides a checklist for compliance with its standards. NIMS is presently developing a credentialing program for particular occupations in homeland security. Called the National Emergency Responder Credentialing System, it will document minimum professional qualifications, certifications, training, and education requirements that define the standards required for specific emergency response functional positions.

Job titles under consideration for the credential program are

- Incident management
- Emergency medical services
- Fire/hazardous materials

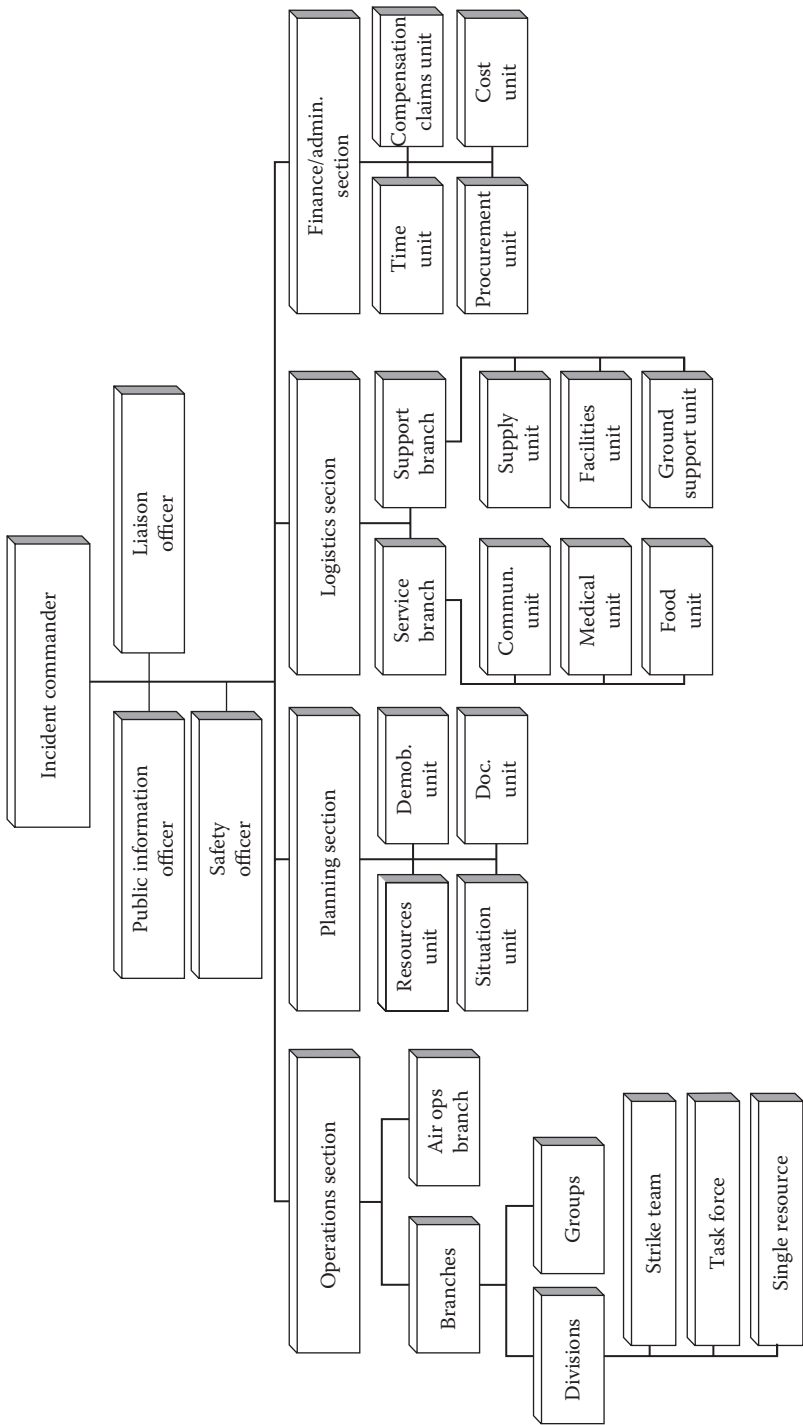


Figure 5.20 ICS organization chart.

Table 5.1 NIMS Class List			
Course Code	Course Title	CEUs	College Credits
IS-3	Radiological Emergency Management-(10/31/2013)	1	n/a
IS-5.a	An Introduction to Hazardous Materials-(10/31/2013)	1	n/a
IS-8.a	Building for the Earthquakes of Tomorrow: Complying with Executive Order 12699-(10/31/2013)	1	1.0
IS-10.a	Animals in Disasters: Awareness and Preparedness-(10/2/2015)	0.4	1.0
IS-11.a	Animals in Disasters: Community Planning-(10/2/2015)	0.4	1.0
IS-15.b	Special Events Contingency Planning for Public Safety Agencies-(10/31/2013)	0.4	1.0**IS-15.b Details
IS-18.20	FEMA EEO Employee Course 2020-(1/6/2020)	0.1	n/a
IS-19.20	FEMA EEO Supervisor Course-2020 (1/6/2020)	0.1	n/a
IS-20.20	Diversity Awareness Course 2020-(1/6/2020)	0.1	1.0**IS-20.20 Details
IS-21.20	Civil Rights and FEMA Disaster Assistance-(1/6/2020)	0.1	1.0**IS-21.20 Details
IS-26	Guide to Points of Distribution-(8/11/2010)	0.4	1.0**IS-26 Details
IS-27	Orientation to FEMA Logistics-(10/31/2013)	0.4	1.0* *IS-27 Details
IS-29.a	Public Information Officer Awareness-(8/5/2019)	0.7	1.0**IS-29.a Details
IS-30.b	Mitigation eGrants System for the Subgrant Applicant-(1/10/2018)	0.3	1.0**IS-30.b Details
IS-31.b	Mitigation eGrants for the Grant Applicant-(1/10/2018)	0.5	1.0**IS-31.b Details

- Law enforcement
- Medical and public health, public works
- Search and rescue

Institutions can be certified as compliant with NIMS standards and requirements (see Figure 5.21).

NIMS fosters interagency cooperation by recognizing the need for mutual aid and cooperation rather than insular turf protection. NIMS encourages governmental entities to enter into formal agreements to assist one another in the event of disaster or a terrorist event. See the sample mutual aid agreement, courtesy of the Minnesota Municipalities Utilities Association, in Figure 5.22.

NIMS CERTIFICATION

Please sign and return this form with your Homeland Security Grant Program

I certify that _____ (Jurisdiction/Tribe/Agency Name) has successfully complied with the following 23 NIMS compliance requirements ("taken as a whole") as directed by the NIMS Integration Center and the U.S. Department of Homeland Security for the Homeland Security Grant Programs.

Jurisdiction Adoption and Infrastructure

- Adopted NIMS at the jurisdictional/tribal/agency level as well as promoted and encouraged jurisdiction-wide adoption.
- Established a planning process to ensure the communication and implementation of NIMS requirements across the jurisdiction. This process must provide a means for measuring progress and facilitate reporting.
- Designated a single point of contact within the jurisdictional government to serve as the principal coordinator for NIMS implementation jurisdiction-wide.
- To the extent permissible by law, ensured that federal preparedness funding to the jurisdiction/tribe/agency is linked to satisfactory progress in meeting the requirements related to FY06 NIMS implementation requirements.
- To the extent permissible by jurisdictional/tribal/agency law, audit agencies, and review organizations routinely included NIMS implementation requirements in all audits associated with federal preparedness grant funds. This process will validate the self-certification process for NIMS compliance.

Command and Management

- Incident Command System (ICS): Managed all emergency incidents and preplanned (recurring/special) events in accordance with ICS organizational structure, doctrine, and procedures, as defined in NIMS. ICS implementation must have included the consistent application of Incident Action Planning and Common Communication Plans.
- Multi-agency Coordination System: Coordinated and supported emergency incident and event management through the development and use of integrated multi-agency coordination systems.
- Public Information System: Institutionalized, within the framework of ICS, the Public Information System, comprising of the Joint Information System (JIS) and a Joint Information Center (JIC). The public Information System ensures an organized, integrated, and coordinated mechanism to perform critical emergency information, crisis communications and public affairs functions which is timely, accurate, and consistent. This includes training for designated participants from the jurisdiction/tribe/agency management and key agencies.

Preparedness: Planning

- Established the jurisdiction's NIMS baseline against the FY05 and FY06 implementation requirements.
- Coordinated and leveraged all federal preparedness funding to implement the NIMS.
- Revised and updated plans and SOPs to incorporate NIMS and National Response Plan (NRP) components, principles and policies, to include planning, training, response, exercises, equipment, evaluation, and corrective actions.
- Promoted intrastate and interagency mutual aid agreements, to include agreements with the private sector and non-governmental organizations.

Preparedness: Training

- Leveraged training facilities to coordinate and deliver NIMS training requirements in conformance with the NIMS National Standard Curriculum.
- Completed IS-700 NIMS: An Introduction

Figure 5.21 NIMS certification.

(Continued)

Homeland Security

- Completed IS-800 NRP: An Introduction
- Completed ICS 100 and ICS 200 Training

Preparedness: Exercises

- Incorporated NIMS/ICS into all regional and jurisdictional training and exercises.
- Participated in an all-hazard exercise program based on NIMS that involves responders from multiple disciplines and multiple jurisdictions.
- Incorporated corrective actions into preparedness and response plans and procedures.

Resource Management

- Inventoried jurisdictional response assets to conform to Homeland Security resource typing standards.
- Developed state plans for the receipt and distribution of resources as outlined in the National Response Plan (NRP) Catastrophic Incident Annex and Catastrophic Incident Supplement.
- To the extent permissible by state and local law, ensured that relevant national standards and guidance to achieve equipment, communication and data interoperability are incorporated into state and local acquisition programs.

Communication and Information Management

- Applied standardized and consistent terminology, including the establishment of plain English communication standards across public safety sector.

(Name & Title of Jurisdictional Official): _____

(Name of Jurisdiction/Tribe/Agency): _____

Signature: _____ Date: _____

Exceptions to the above (please list): _____

Figure 5.21 (*CONTINUED*) NIMS certification.

The ICS plays a central role in the publication of NIMS forms and publications and educational materials. NIMS, as part of its mission, seeks out its constituencies with an educational aim.

The ICS is charged with the management of resources relating to a given incident. NIMS establishes requirements for inventory and the mobilization, dispatch, tracking, and recovery of resources over the life cycle of an incident. In addition, NIMS provides a standardized protocol for all communications and media at every level of incident management, including the sharing of information among all interested agencies, the implementation of interoperable communication systems, and the storage and management of information relating to the incident (see Figure 5.23⁴¹).

Internet Exercise: To access the entire NIMS guide, published by FEMA, see <http://www.fema.gov/nims-doctrine-supporting-guides-tools>.

NIMS is an ongoing process with improvements, refinements, and adjustments occurring on a regular basis. From another perspective, NIMS builds on its infrastructure year by year. NIMS, being of relatively young design, learns from both its successes and failures. In directing agencies to implement the program, it looks not only to the present requirements but also to past demands and future expectations. NIMS methodology was heavily updated in 2017.⁴² NIMS expects the agency to track its history and trace its evolution in the process. See Figure 5.24⁴³ for this historical approach.

FEMA also publishes an activity schedule for particular settings like schools and hospitals. See Figure 5.25.⁴⁴

MUTUAL AID AGREEMENT

In consideration of the mutual commitments given herein each of the Signatories to this Mutual Aid Agreement agrees to render aid to any of the other Signatories as follows:

- 1. Request for aid. The Requesting Signatory agrees to make its request in writing to the Aiding Signatory within a reasonable time after aid is needed and with reasonable specificity. The Requesting Signatory agrees to compensate the Aiding Signatory as specified in this Agreement and in other agreements that may be in effect between the Requesting and Aiding Signatories.
- 2. Discretionary rendering of aid. Rendering of aid is entirely at the discretion of the Aiding Signatory. The agreement to render aid is expressly not contingent upon a declaration of a major disaster or emergency by the federal government or upon receiving federal funds.
- 3. Invoice to the Requesting Signatory. Within 90 days of the return to the home work station of all labor and equipment of the Aiding Signatory, the Aiding Signatory shall submit to the Requesting Signatory an invoice of all charges related to the aid provided pursuant to this Agreement. The invoice shall contain only charges related to the aid provided pursuant to this Agreement.
- 4. Charges to the Requesting Signatory. Charges to the Requesting Signatory from the Aiding Signatory shall be as follows:
 - a. Labor force. Charges for labor force shall be in accordance with the Aiding Signatory's standard practices.
 - b. Equipment. Charges for equipment, such as bucket trucks, digger derricks, and other special equipment used by the Aiding Signatory, shall be at the reasonable and customary rates for such equipment in the Aiding Signatory's location.
 - c. Transportation. The Aiding Signatory shall transport needed personnel and equipment by reasonable and customary means and shall charge reasonable and customary rates for such transportation.
 - d. Meals, lodging, and other related expenses. Charges for meals, lodging, and other expenses related to the provision of aid pursuant to this Agreement shall be the reasonable and actual costs incurred by the Aiding Signatory.
- 5. Counterparts. The Signatories may execute this Mutual Aid Agreement in one or more counterparts, with each counterpart being deemed an original Agreement, but with all counterparts being considered one Agreement.
- 6. Execution. Each party hereto has read, agreed to, and executed this Mutual Aid Agreement on the date indicated.

Date _____ Entity _____
_____ By _____
Title _____

Figure 5.22 Mutual aid agreement.

5.9 Conclusion

Identifying risk, threats, and hazards is the first piece in the homeland security puzzle. Homeland security professionals must prepare, plan for, and respond to these potential risks. Hence, the role of training and exercises that anticipate these harms is crucial in any homeland security plan. DHS stresses training for all eventualities, as evidenced through its organizational structure, budgets and grants, and core competencies. The DHS Office of G&T is the funding mechanism for training and grants. DHS coordinates major training events, at a national scale through its TOPOFF program and the National Exercise Plan programs. The emergency side of homeland

Homeland Security

Incident Radio Communications Plan			1. INCIDENT NAME	2. DATE/TIME PREPARED	3. OPERATIONAL PERIOD DATE/TIME
4. BASE RADIO CHANNEL UTILIZATION					
SYSTEM/CACHE	CHANNEL	FUNCTION	FREQUENCY/TONE	ASSIGNMENT	REMARKS
5. PREPARED BY (COMMUNICATIONS UNIT)					

Figure 5.23 Incident radio communications plan.

training is centered at EMI, which delivers a bevy of programs for first responders and other emergency professionals. EMI uses residential, online and independent study methodologies for instruction. In the world of WMD, the CDP-the Center for Domestic Terrorism, is considered the key trainer. All training for homeland security is evaluated by HSEEP, which delivers standardized methodology and terminology for exercise design, development, and planning. HSEEP regularly promulgates best practices for the homeland security industry. Specialized training for critical infrastructure holds a prominent place in the training portion of the homeland mission. Other training modalities include the HSDL, LLIS, AARs, CERTs, and NIMS—a planning process for institutions, in both the private and the public sectors, that anticipates threat and hazard.

How homeland security professionals respond to and recover from threats and hazards is keenly dealt with in this chapter. Response is how government attends to the event in an immediate sense. The lessons learned from both Hurricane Katrina and Hurricane Sandy say much about the importance of response. DHS publishes a National Response Framework (NRF) to guide homeland and governmental agencies. The framework stresses the need to partner and work collaboratively, the necessity for layers of government to work in unity, the recognition that one command will corral these various constituencies, and that flexibility and readiness in response are central to the mission.

Keywords

After-Action Reports; Assistance to Firefighters Grant; Best Practices; Center for Domestic Preparedness; Chemical, Ordnance, Biological, and Radiological Training Facility; Community Emergency Response Teams; Compliance Standards; Continuing Education; Credentialing; Disaster Field Training Organization; Disaster Preparedness; Discussion-Based Exercises;



NIMS IMPLEMENTATION ACTIVITY SCHEDULE

The matrix below summarizes by Federal Fiscal Year (FY) all on-going NIMS implementation activities that have been prescribed by the NIMS Integration Center in FYs 2005 and 2006, as well as the **seven** new activities for States and territories and **six** new activities for tribes and local jurisdictions required in FY 2007.

State, territorial, tribal, and local jurisdictions should bear in mind that implementation activities from previous fiscal years remain on-going commitments in the present fiscal year. Jurisdictions must continue to support all implementation activities required or underway in order to achieve NIMS compliance.

Future refinement of the NIMS will evolve as policy and technical issues are further developed and clarified. As a result, the NIMS Integration Center may issue additional requirements to delineate what constitutes NIMS compliance in FY 2008 and beyond. With the completion of the FY 2007 activities, State, territorial, tribal and local jurisdictions will have the foundational support for future NIMS implementation and compliance. The effective and consistent implementation of the NIMS nationwide will result in a strengthened national capability to prevent, prepare for, respond to and recover from any type of incident.

NIMS IMPLEMENTATION ACTIVITY		FY 2007		FY 2006		FY 2005	
		STATE/ TERRITORY	TRIBAL/ LOCAL	STATE/ TERRITORY	TRIBAL/ LOCAL	STATE/ TERRITORY	TRIBAL/ LOCAL
ADOPTION	1. Support the successful adoption and implementation of the NIMS.					✓	✓
	2. Adopted NIMS for all government departments and agencies; as well as promote and encourage NIMS adoption by associations, utilities, non-governmental organizations (NGOs) and private sector incident management and response organizations.			✓	✓		
	3. Monitor formal adoption of NIMS by all tribal and local jurisdictions.			✓			
	4. Establish a planning process to ensure the communication and implementation of NIMS requirements, thereby providing a means for measuring progress and facilitate reporting.			✓			
	5. Designate a single point of contact to serve as the principal coordinator for NIMS implementation.		✓	✓			
	6. Designate a single point of contact within each of the jurisdiction's Departments and Agencies.	✓					
	7. To the extent permissible by law, ensure that Federal preparedness funding, including DHS Homeland Security Grant Program and the Urban Areas Security Initiative (UASI), support NIMS implementation at the State and local levels and incorporate NIMS into existing training programs and exercises.					✓	
	8. To the extent permissible by law, ensure that federal preparedness funding to State and territorial agencies and tribal and local jurisdictions is linked to satisfactory progress in meeting FY2006 NIMS implementation requirements.			✓			
	9. To the extent permissible by State and territorial law and regulations, audit agencies and review organizations routinely include NIMS implementation requirements in all audits associated with federal preparedness grant funds, validating the self-certification process for NIMS compliance.			✓			
	10. Monitor and assess outreach and implementation of NIMS Requirements.	✓					
COMMAND AND MANAGEMENT	11. Coordinate and provide technical assistance to local entities regarding NIMS institutionalized use of ICS.					✓	
	12. Manage all emergency incidents and pre-planned (recurring/special) events in accordance with ICS organizational structures, doctrine and procedures, as defined in NIMS. ICS implementation must include the consistent application of Incident Action Planning and Common Communications Plans.			✓	✓		
	13. Coordinate and support emergency incident and event management through the development and use of integrated multi-agency coordination systems, i.e. develop and maintain connectivity capability between local Incident Command Posts (ICP), local 911 Centers, local Emergency Operations Centers (EOCs), the state EOC and regional and federal EOCs and NRP organizational elements.			✓	✓		
	14. Institutionalize, within the framework of ICS, the Public Information System (PIS), comprising of the Joint Information System (JIS) and a Joint Information Center (JIC).			✓	✓		
	15. Establish public information system to gather, verify, coordinate, and disseminate information during an incident.	✓	✓				
PREPAREDNESS: PLANNING	16. Establish NIMS baseline against the FY 2005 and FY 2006 implementation requirements.			✓	✓		
	17. Develop and implement a system to coordinate and leverage all federal preparedness funding to implement the NIMS.			✓	✓		
	18. Incorporate NIMS into Emergency Operations Plans (EOP).					✓	
	19. Revise and update plans and SOPs to incorporate NIMS and National Response Plan (NRP) components, principles and policies, to include planning, training, response, exercises, equipment, evaluation and corrective actions.			✓	✓		
	20. Promote intrastate mutual aid agreements, to include agreements with private sector and non-governmental organizations.					✓	✓
PREPAREDNESS: TRAINING	21. Participate in and promote intrastate and interagency mutual aid agreements, to include agreements with the private sector and non-governmental organizations.			✓	✓		
	22. Leverage training facilities to coordinate and deliver NIMS training requirements in conformance with the NIMS National Standard Curriculum.			✓			
	23. Complete training—IS-700 NIMS: An Introduction, IS-800 NRP: An Introduction; ICS-100 and ICS-200.			✓	✓		
	24. Complete training—ICS-300, ICS-400.	✓	✓				
PREPAREDNESS: EXERCISES	25. Incorporate NIMS/ICS into training and exercises.					✓	✓
	26. Participate in an all-hazard exercise program based on NIMS that involves responders from multiple disciplines and multiple jurisdictions.			✓	✓		
	27. Incorporate corrective actions into preparedness and response plans and procedures.			✓	✓		
	28. Inventory response assets to conform to FEMA Resource Typing standards.			✓	✓		
RESOURCE MANAGEMENT	29. Develop state plans for the receipt and distribution of resources as outlined in the National Response Plan (NRP) Catastrophic Incident Annex and Catastrophic Incident Supplement.			✓			
	30. To the extent permissible by state and local law, ensure that relevant national standards and guidance to achieve equipment, communication and data interoperability are incorporated into state and local acquisition programs.			✓	✓		
	31. Validate that inventory of response assets conforms to FEMA Resource Typing Standards.	✓	✓				
	32. Utilize response asset inventory for mutual aid requests, exercises, and actual events.	✓	✓				
COMMUNICATION MANAGEMENT	33. Apply standardized and consistent terminology, including the establishment of plain language communications standards across public safety sector.			✓	✓		
	34. Develop systems and processes to ensure that incident managers at all levels share a common operating picture of an incident.	✓	✓				

October 2006

Figure 5.24 NIMS implementation activity schedule.

Homeland Security

CHECKLIST: NIMS IMPLEMENTATION ACTIVITIES FOR SCHOOLS AND HIGHER EDUCATION INSTITUTIONS (HEIs)		
COMPONENT	IMPLEMENTATION ACTIVITY	STATUS
ADOPTION	1. Adopt NIMS at the school and campus community level.	Complete ☐
		Not Complete ☐
		In Progress ☐
COMMAND AND MANAGEMENT	2. Institutionalize the Incident Command System (ICS) for managing all emergency incidents and pre-planned school and campus events.	Complete ☐
		Not Complete ☐
		In Progress ☐
	3. Coordinate and support the development and use of integrated Multi-agency Coordination Systems (MACS).	Complete ☐ Not Complete ☐ In Progress ☐
PREPAREDNESS: PLANNING	4. Establish the Public Information System (PIS) within the ICS framework.	Complete ☐
		Not Complete ☐
		In Progress ☐
	5. Establish NIMS strategy and timeline for full implementation.	Complete ☐ Not Complete ☐ In Progress ☐
PREPAREDNESS: TRAINING	6. Develop and implement a system to coordinate and leverage Federal preparedness funding to implement NIMS.	Complete ☐
		Not Complete ☐
		In Progress ☐
	7. Update emergency management plans to incorporate NIMS and reflect National Response Framework.	Complete ☐ Not Complete ☐ In Progress ☐
PREPAREDNESS: EXERCISES	8. Participate in and promote mutual aid agreements.	Complete ☐
		Not Complete ☐
		In Progress ☐
	9. Key school and campus personnel complete NIMS training.	Complete ☐ Not Complete ☐ In Progress ☐
RESOURCE MANAGEMENT	10. Incorporate NIMS and ICS into all emergency management training and exercises.	Complete ☐
		Not Complete ☐
		In Progress ☐
	11. Participate in an all-hazard exercise program based on NIMS that involves first responders from multiple disciplines and jurisdictions.	Complete ☐ Not Complete ☐ In Progress ☐
COMMUNICATION & INFORMATION MANAGEMENT	12. Incorporate corrective actions into preparedness and response plans and procedures.	Complete ☐
		Not Complete ☐
		In Progress ☐
	13. Maintain an inventory of organizational response assets—equipment, resources, and supplies.	Complete ☐ Not Complete ☐ In Progress ☐
RESOURCE MANAGEMENT	14. To the extent permissible by law, ensure that relevant national standards and guidance to achieve equipment, communication, and data interoperability are incorporated into acquisition programs.	Complete ☐
		Not Complete ☐
		In Progress ☐
	15. Apply standardized and consistent terminology for school and campus incidents, including the establishment of plain English communication standards across the public safety sector.	Complete ☐ Not Complete ☐ In Progress ☐

Figure 5.25 The NIMS Implementation Activities Checklist for schools and Higher Education Institutions (HEIs).

Emergency Management Institute; EMI Independent Study Program; Fire Prevention and Safety Grant; Fire Safety; Homeland Security Exercise and Evaluation Program; HSEEP Exercises; Incident Command System; In-Service Training; Lessons Learned Information Sharing; National Domestic Preparedness Consortium; National Emergency Responder

Credentialing System; National Incident Management System; National Integration Center; NIMS Certification; Office of Grants and Training; Operations-Based Exercises; Residential Training Facility; Search and Rescue; TOPOFF Exercise; U.S. Fire Administration

Discussion Questions

1. Discuss the importance of training in the world of homeland security.
2. Critics of DHS frequently cite the agency's tendency to bite off more than it can chew. In the area of training, is this legitimate?
3. Explain the critical function of EMI.
4. Why did DHS design and implement HSEEP?
5. Discuss how homeland professionals train for the protection of critical infrastructure.
6. Of what import is the LLIS program? How does such a program benefit homeland leaders?
7. What are the general goals of NIMS?
8. Why is it essential that an ICS be implemented?
9. What is the value of a NIMS certification program?
10. Explain the philosophy of the NRF. In particular, comment on why shared responsibility is so important in the NRF.

Practical Exercises

1. Collect and collate a NIMS file. Prepare an index of these documents.
2. Draft a NIMS implementation plan for your place of work. Use the FEMA template for the implementation at <https://www.fema.gov/planning-templates>.
3. Contact your statewide DHS office. Determine whether a TOPOFF exercise will occur in your region.
4. Contact a local police department. Find out if that office has applied for DHS training funds.
5. Write to EMI for a course catalog.
6. Find out where CERTs exist in your area.

Notes

- 1 FEMA, Grants Management, <https://training.fema.gov/grantsmanagement/> (accessed August 11, 2020).
- 2 DHS, FEMA, Office of G&T, G&T Mission, <http://ojp.gov/funding/> (accessed August 11, 2020).
- 3 FEMA, *Grant Programs Directorate Strategic Plan, FY 2009–2010*, October 9, 2008.
- 4 Ibid. See also: Dept. of Homeland Security, Science & Technology, Grants Resources, <https://www.dhs.gov/science-and-technology/frg-grants> (accessed August 11, 2020).

Homeland Security

- 5 FEMA, Types of Grants, <https://www.fema.gov/grants> (accessed August 11, 2020).
- 6 Ibid.
- 7 Office of the President, *Homeland Security Presidential Directive 8*, December 17, 2003.
- 8 DHS press release, DHS announces grant allocations for fiscal year (FY) 2015 preparedness grants (July 28, 2015), <http://www.dhs.gov/news/2015/07/28/dhs-announces-grant-allocations-fiscal-year-fy-2015-preparedness-grants> (accessed August 22, 2020).
- 9 FEMA, National Level Exercise 2018, https://www.fema.gov/media-library-data/1531511400452-4a423adc2367a43386699d3827f100d3/NLE_Infograph.pdf (accessed August 11, 2020).
- 10 DHS, *Fact Sheet: National Level Exercise 2012* (June 5, 2012), <https://www.dhs.gov/news/2012/06/05/fact-sheet-national-level-exercise-2012> (accessed August 11, 2020); FEMA, *National Level Exercise 2012 Quick Look Report* (March 2013), http://www.fema.gov/media-library-data/20130726-1911-25045-9856/national_level_exercise_2012_quick_look_report.pdf (accessed August 11, 2020).
- 11 See M. Paddock, Get your fire grants while they last, *Homeland Security Today*, August 2011: 8.
- 12 FEMA, Center for Domestic Preparedness, Find Training, <https://cdp.dhs.gov/find-training> (accessed August 11, 2020).
- 13 See: FEMA, Center for Domestic Preparedness, About, <https://cdp.dhs.gov/about> (accessed August 11, 2020).
- 14 FEMA, EMI, History, https://training.fema.gov/docs/emi_annual_report-fy2018.pdf (accessed August 11, 2020).
- 15 FEMA, EMI, Disaster Field Training Operations, Mission, <https://training.fema.gov/programs/dfto> (accessed August 11, 2020).
- 16 FEMA, EMI, History, <https://training.fema.gov/history.aspx> (accessed August 11, 2020).
- 17 FEMA, EMI, EMI School Program, <https://training.fema.gov/programs/emischool/emischool.aspx> (accessed August 11, 2020); W. D. Jones, Recruiting future safety professionals, *Professional Safety*, 60 (2015): 22.
- 18 DHS, Critical Infrastructure Sectors, <http://www.dhs.gov/critical-infrastructure-sectors> (accessed August 11, 2020); Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience, (February 12, 2013), <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (accessed August 11, 2020).
- 19 Practitioners are generally favorable to the reality-based exercise. HSEEP stress that sort of training as well as scenario-based learning. See D. R. Hales and P. Race, Applying a framework of defining emergency management scenarios, *Journal of Emergency Management*, 9 (2011): 15.
- 20 FEMA, Homeland Security Exercise and Evaluation Program (HSEEP) 2020 Revision, <https://www.fema.gov/media-library-data/1582303013530-0281b8d216648f8e4b3bfad1c9d6ebe2/HSEEP-Information-Sheet-20200203.pdf> (accessed August 2020).
- 21 DHS, *Homeland Security Exercise and Evaluation Program (HSEEP)*, vi (April 2013), <https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf> (accessed August 11, 2020).
- 22 FEMA, HSEEP Participant Guide, <https://dem.nv.gov/uploadedFiles/demnv.gov/content/raining/HSEEP%20GUIDE%20-%20Module%202.pdf> (accessed August 11, 2020).
- 23 Ibid.
- 24 DHS, *Homeland Security Exercise and Evaluation Program (HSEEP)*, TABLE 2.9 AT PAGE 2.11 (April 2013), <https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf> (accessed August 11, 2020).
- 25 DHS, *Homeland Security Exercise and Evaluation Program (HSEEP)*, 3.12 (April 2013), <https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf> (accessed August 11, 2020).
- 26 DHS, *Homeland Security Exercise and Evaluation Program (HSEEP)*, 2.4 (April 2013), <https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf> (accessed August 11, 2020).
- 27 FEMA, LLIS program, <https://www.fema.gov/lessons-learned-information-sharing-program> (accessed August 11, 2020).

- 28 See: CISA, SLTT Governance Guide Working Group: Meeting 8, <https://www.cisa.gov/safecom/blog/2018/09/24/slitt-governance-guide-working-group-meeting-8> (accessed August 11, 2020).
- 29 R. Kelly, 10 Years after 9/11: Lessons learned by the New York City Police Department, *Police Chief*, September 2011: 20–25.
- 30 Naval Postgraduate School, Center for Homeland Defense and Security, Homeland Security Digital Library, <https://www.hsdl.org/c> (accessed August 11, 2020).
- 31 Homeland Security Digital Library, COVID-19 Resource Archive, <https://www.hsdl.org/a/covidarchive/> (accessed August 11, 2020).
- 32 See: FEMA, CERT Basic Training Participant Manual, https://www.ready.gov/sites/default/files/2019.CERT_.Basic_.PM_FINAL_508c.pdf (accessed August 11, 2020).
- 33 US Dept of Homeland Security, Community Emergency Response Team, <https://www.ready.gov/cert/> (accessed August 11, 2020).
- 34 A. I. Anderson, D. Compton, and T. Mason, Managing in a dangerous world: The National Incident Management system, *Engineering Management Journal* 16(3) (2004): 114.
- 35 Office of the President, *Homeland Security Presidential Directive 5*, February (2003): 3.
- 36 See: FEMA, National Incident Management System Training Program, (May 2020), https://www.fema.gov/media-library-data/1589909305523-a2able0198f83e85a6ab766ccf0e7efc/NIMS_Training_Program_FINAL.pdf (accessed August 11, 2020).
- 37 See: FEMA, National Incident Management System, <https://www.fema.gov/national-incident-management-system> (accessed August 11, 2020).
- 38 In 2010, by way of illustration, the NIMS compliance standards were published and can be found here for reference: FEMA, FY 2010 NIMS Implementation Objectives and Metrics for Federal Departments and Agencies, https://www.fema.gov/pdf/emergency/nims/FY2010_FederalNIMSImplementationObjectivesMetrics.pdf (accessed August 11, 2020).
- 39 ICS Organization, <https://training.fema.gov/emiweb/is/icsresource/assets/ics%20organizational%20structure%20and%20elements.pdf> (accessed August 11, 2020).
- 40 FEMA, Emergency Management Institute, ISP Courses, <https://training.fema.gov/is/crslist.aspx> (accessed August 11, 2020).
- 41 See also: Unit 4: NIMS Communications and Information Management, http://video.stpsb.org/media/Curriculum/fema/student_nims_communication.pdf (accessed August 11, 2020).
- 42 See: FEMA EMI, National Incident Management System (NIMS) 2017 Learning Materials, <https://training.fema.gov/nims/docs/nims.2017.instructor%20student%20learning%20materials.pdf> (accessed August 11, 2020).
- 43 FEMA, NIMS Implementation Activity Schedule, https://www.fema.gov/pdf/emergency/nims/nims_imp_act.pdf (accessed August 11, 2020).
- 44 FEMA, Checklist: NIMS Implementation Activities for Schools and Higher Education Institutions (HEIS), https://www.education.ne.gov/wp-content/uploads/2017/07/ChecklistNIMS_ImplementationActivitiesFinal.pdf (accessed August 11, 2020).



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

DHS Challenges: National versus State and Local, National Security versus Homeland Security

OBJECTIVES

1. To evaluate the various national, state, and local relationships relating to homeland security that exist in U.S. government agencies
2. To compare and contrast homeland security agencies at the state level, including their organization, policies, and operating parameters
3. To analyze the many types of homeland security task forces and commissions that exist at the state level
4. To describe the homeland security structures that are in place at the local level and analyze the differences that arise in major metropolitan, urban, suburban, and rural areas
5. To describe fusion centers, their purpose, staffing, and locations
6. To explain the various funding programs available from the federal government for state and local homeland security initiatives
7. To describe current military initiatives specifically relating to homeland security intelligence gathering
8. To describe current military initiatives specifically relating to specialized units dedicated to homeland security and the identification and tracking of weapons of mass destruction (WMDs)

6.1 Introduction

From its earliest conception, the authors of a national Department of Homeland Security (DHS) envisioned the widespread participation of states and localities as the programs and policies of homeland security were implemented. As early as 2004, the shift away from centralized

Homeland Security

authority had taken root in the culture of homeland security. The department's own *Report from the Task Force on State and Local Homeland Security Funding* unequivocally endorses not only local involvement but local control. In addition, it urges policymakers to author policy from the ground level up rather than it being descended from DHS itself.

Those at the municipal, state, tribal and federal level responsible for using these funds have a better understanding of what each needs to do to achieve success. Recommendations for major changes would have only added confusion where clarity is emerging. It is our belief that these recommended actions coupled with expected maturity of the program will result in measurable progress towards making the nation safer, stronger, and better.¹

The federal government, despite its agency status, cannot carry out the local and regional field requirements of DHS, nor would it be wise to over centralize these diverse functions. If history elucidates anything, it is that DHS and its size directly correlate to its level of effectiveness. The larger the enterprise gets, the more an unmanageable beast it becomes. At the outset of DHS, there was an unequivocal understanding concerning shared responsibilities in these matters. Early in the life of DHS, there was full recognition of the necessity of federal, state, and local interaction. Under the DHS Office of Intelligence and Analysis, there is a structure for such reporting under the "State and Local Program Office" slot (see Figure 6.1).

The National Governors' Association has taken the lead in the statewide role, especially by and through its National Governors' Association (NGA) Center for Best Practices (Figure 6.2²).

Intelligence, in order to have any significant meaning in homeland defense (HD), must be naturally and continuously shared rather than protected or hidden due to bureaucratic layers of multiple agencies. Intelligence is the best and most telling example of how important the interaction between state, federal, and local authorities is and must be.³ President Bush, when recommending the establishment of DHS, wanted to set a tone and mission for the new federal agency. He did, however, allow for states to maintain autonomy as well as have a mechanism for input. By his presidential directive, it was clear that a collaborative and integrative approach in the application of homeland security was the intended goal. Bush noted

The Federal Government recognizes the roles and responsibilities of State and local authorities in domestic incident management. Initial responsibility for managing domestic incidents generally falls on State and local authorities. The Federal Government will assist State and local authorities when their resources are overwhelmed, or when Federal interests are involved. The Secretary will coordinate with State and local governments to ensure adequate planning, equipment, training, and exercise activities. The Secretary will also provide assistance to State and local governments to develop all-hazards plans and capabilities, including those of greatest importance to the security of the United States, and will ensure that State, local, and Federal plans are compatible.⁴

Internet Exercise: Become familiar with the nature and structure of our 50 state centers for homeland security by visiting <https://www.nga.org/center/issues/governors-homeland-security-advisors-council/>.

6.2 Challenge of National Policy at the State and Local Levels

DHS has always fully understood the necessity for fruitful and productive relationships with state and local authorities. By setting up the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), DHS sought the membership of those in the state and local trenches. Membership criteria included

- A state, local, tribal, or territorial homeland security director or equivalent with relevant programmatic planning and operational responsibilities

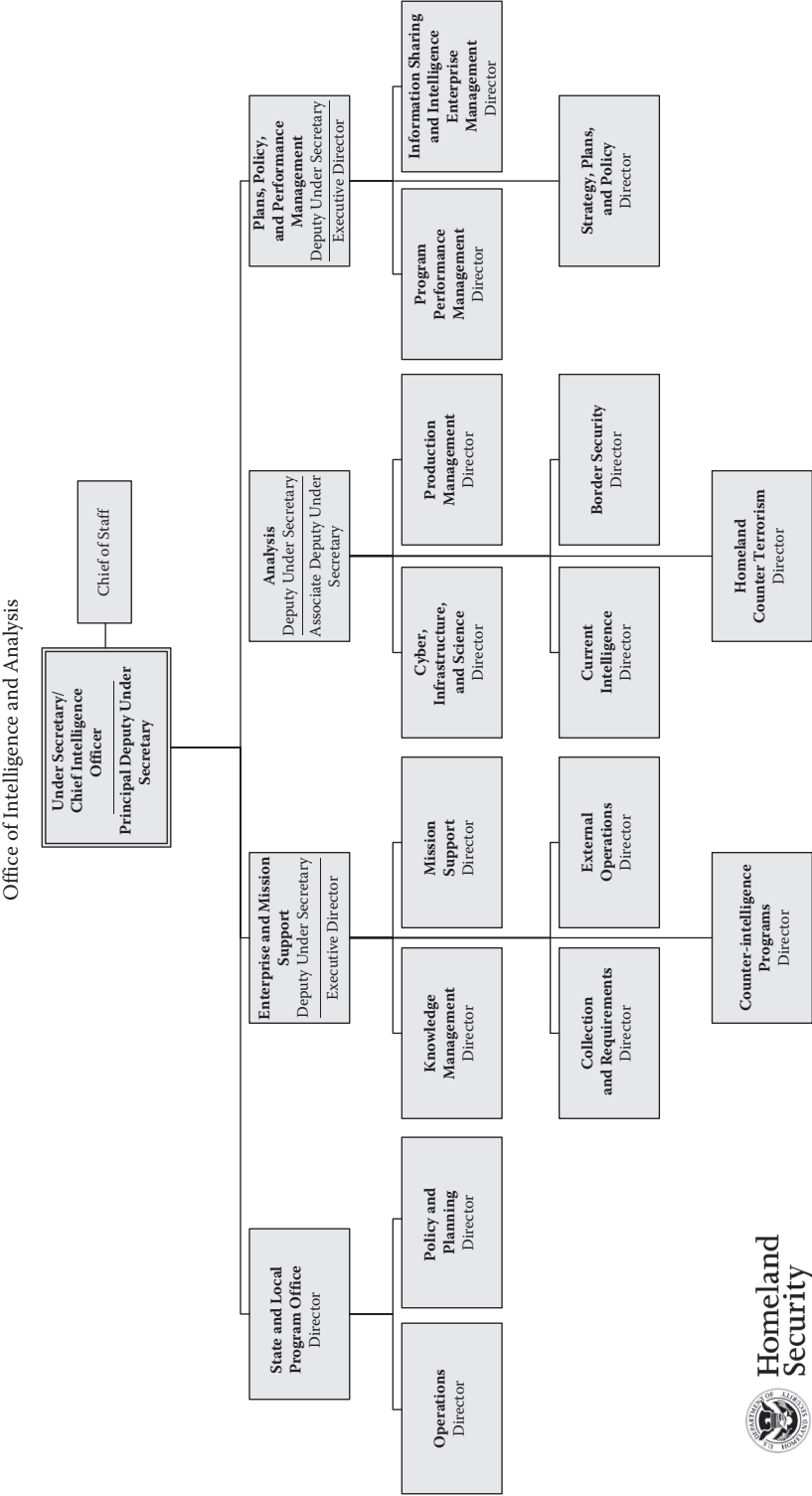


Figure 6.1 Department of Homeland Security, Office of Intelligence, and Analysis Organizational Chart.





Figure 6.2 National Governors’ Association Center for Best Practices logo.

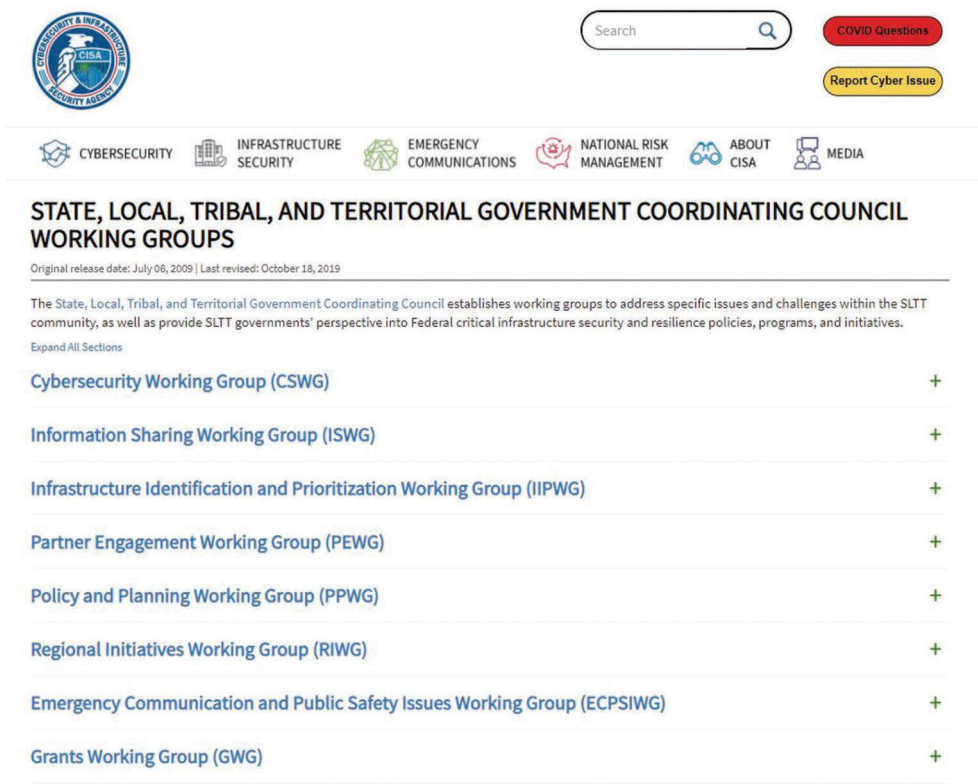


Figure 6.3 State, Local, Tribal, and Territorial Government Coordinating Council working groups.

- Accountable for the development, improvement, and maintenance of critical infrastructure protection policies or programs at the state, local, or tribal level
- Recognized among his or her peers as a leader
- Committed to acting as national representative regarding homeland practices relevant to states and localities

The council conducts much of its business through working groups, charted in Figure 6.3.⁵

Hence, while policy making emanates from the federal system, management inevitably falls to the states and localities. How these policies are carried out, and whether they can be carried out, is a question more appropriate for the local level.

6.2.1 Structure at the State Level

Relevant departments and agencies of the federal government must take the lead in implementing this system, while state and local governments must implement and adopt homeland policies

6.2 Challenge of National Policy at the State and Local Levels

consistent with DHS policy. State homeland security entities were created to ensure that states were prepared at the frontlines for terrorist attacks. State entities provide a structural entity for a mission of state protections by coordinating the various needs of the governor's office, the homeland security director, the state emergency management office, other state agencies, local governments, the private sector, volunteer organizations, and the federal government. Every state erected an Office of Homeland Security soon after 9/11. The current compendium includes those offices shown in Figure 6.4.

How states choose to construct their Offices of Homeland Security is unique to the given jurisdiction. Most states rely on the governor to designate a person to be a homeland security director. The position is advisory panel and agency driven, as well as the office where related functions of homeland security are coordinated, such as emergency management, law enforcement, health, and related public safety functions. To see a common design, review the example from Louisiana in Figure 6.5.⁶

Some states tackle the many demands of homeland security better than others. To be certain, New York State, due to its 9/11 connection and having an already highly trained law enforcement emergency community, represents a splendid example of skill and determination in the defense of the homeland and the active prevention of terror.⁷ Aside from this traditional outlook, New York State has done a very effective job in dealing with the risk and emergency side of things. The entire state has been broken down into response regions for emergency purposes (see Figure 6.6).⁸ The state also has an exceedingly clear picture of the aims and goals of its homeland office and agency. See Figure 6.7⁹ for its 2020 summary.

Other designs incorporate existing offices at the state level, such as the adjutant general, the National Guard, or specialized task forces that are composed of executive office staff and agency heads from law enforcement, fire and rescue, public health, and public works.

States are increasingly being asked to assume more under homeland security protocols. For some, the farther away from federal control the process is, the more effective. Both the states and DHS itself realize the necessity of state and local influence and allots a sizable portion of government funding to advance this ambition by grants and other funding mechanisms. Even the states themselves budget for various homeland functions. See Table 6.1¹⁰ for a summary chart, state by state, of funds allotted for homeland purposes.

Tennessee, for example, has a sophisticated network of homeland programs and personnel carrying out the homeland mission. Its overall purpose is as follows:

The Tennessee Office of Homeland Security has the primary responsibility and authority for directing statewide activities pertaining to the prevention of, and protection from, terrorist-related events. This responsibility includes the development and implementation of a comprehensive and coordinated strategy to secure the state from terrorist threats and attacks. Further, the office of Homeland Security serves as a liaison between federal, state, and local agencies, and private sector on matters relating to the security of our state and citizens.

- AWARENESS: Identify and understand terrorist threats within Tennessee.
- PREVENTION: Detect, deter, and mitigate terrorist threats to Tennessee.
- PROTECTION: Safeguard our citizens, their freedoms, property, and the economy of Tennessee from acts of terrorism.
- RESPONSE: Assist in coordinating the response to terrorist-related events.
- ORGANIZATIONAL EXCELLENCE: Putting the safety of our citizens first.¹¹

As in other jurisdictions, Tennessee sets out to educate its citizens and to play an instrumental role in the prevention of and protection of its citizens from terror and its threats.¹² It also publishes and adopts protocols for the more typical threats likely to be encountered. An example, in Figure 6.8,¹³ deals with cyber-safety threats.

Task forces and commissions play a central role in state homeland policy since the composition of these bodies tends to include major players in law enforcement and emergency preparedness.

Homeland Security

State Homeland Security Contacts						
Alabama	Shirrell Roberts	Alabama Department of Homeland Security	PO BOX 1471	Montgomery, Ala. 36130-4115	334-517-2812	www.alea.gov
	Director					
Alaska	Paul Nelson	Alaska Division of Homeland Security &	P.O. Box 5750 Bldg. 49000, Suite B-214	Ft. Richardson, Alaska 99505	907-428-7000	ready.alaska.gov
	Director					
Arizona	Gilbert M. Orrantia	Arizona Department of Homeland Security	1700 West Washington Street,	Phoenix, Ariz. 85007	602-542-7013	http://www.azdohs.gov/
	Director					
Arkansas	AJ Gary	Arkansas Department of Emergency Management	Building 9501	North Little Rock, Ark. 72119-9600	501-683-6700	www.adem.arkansas.gov
	Director		Camp Robinson			
California	Mark Ghilarducci	CAL OES Governor's Office of Emergency Services	3650 Schriever Avenue	Mather, Calif. 95655	916-845-8510	www.caloes.ca.gov
	Acting Secretary					
Colorado	Kevin R. Klein	Colorado Division of Homeland Security &	9195 E. Mineral Avenue, Suite 200	Centennial, CO 80112	720-852-6600	https://www.colorado.gov/dhsem
	Director					
Connecticut	William J. Hackett	Department of Emergency Services and Public	1111 Country Club Rd	Middletown CT 06457	860-685-8531	https://portal.ct.gov/DEMHS
	Emergency Management Director					
Delaware	Kimberly Chandler	Department of Safety and Homeland Security	303 Transportation Circle	Dover, Del. 19903	302-744-2680	http://dshs.delaware.gov/
	Cabinet Secretary		P.O. Box 818			
District of Columbia	Chris Rodriguez	Homeland Security and Emergency Management	2720 Martin Luther King Jr. Avenue, SE	Washington, D.C. 20032	202-727-6161	www.hsema.dc.gov
	Director					
Florida	Jared Moskowitz	Florida Division of Emergency Management	2555 Shumard Oak Boulevard	Tallahassee, Fla. 32399-2100	850-815-4000	https://www.floridadisaster.org/
	Director					
Georgia	Homer Bryson	Georgia Emergency Management /Homeland	P.O. Box 18055	Atlanta, Ga. 30316-0055	404-635-7000	https://gema.georgia.gov/
	Director					
Hawaii	Major Geneal Kenneth Hara	Hawaii Emergency Management Agency	3949 Diamond Head Rd.	Honolulu, Hawaii 96816-4495	808-733-4300	https://dod.hawaii.gov/hiema/
	Director					
Idaho	William B. (Brad) Richy	Office of Emergency Management	4040 West Guard Street, Bldg 600	Boise, Idaho 83705-5004	208-422-3040	https://ioem.idaho.gov/
	Director					
Illinois	Alicia Tate-Nadeau	Illinois Emergency Management Agency	2200 South Dirksen Parkway	Springfield, Ill. 62703	217-782-2700	https://www2.illinois.gov/ema/Pages/default.aspx
	Director					
Indiana	Stephen Cox	Indiana Department of Homeland Security	Indiana Government Center South 302 W. Washington Street, Rm. E208	Indianapolis, Ind. 46204	317-232-2222	http://www.in.gov/dhs/
	Executive Director					
Iowa	V. Joyce Flinn	Homeland Security and Emergency Management	7900 Hickman Road, Suite 500	Windsor Heights, IA 50324	515-725-3231	https://www.homelandsecurity.iowa.gov/
	Director					
Kansas	Maj. Gen. David Weishaar	Division of Emergency Management	2800 SW Topeka Blvd.	Topeka, Kan. 66611	785-646-2000	http://www.kansasastag.gov/kdem_default.asp
	Director					
Kentucky	Josh Keats	Kentucky Office of Homeland Security	200 Mero Street	Frankfort, Ky. 40622	502-564-2081	http://homelandsecurity.ky.gov/
	Executive Director					
Louisiana	James Waskom	Governor's Office of Homeland Security and	7667 Independence Blvd	Baton Rouge, La. 70806	225-925-7500	www.gohsep.la.gov
	Director					
Maine	Anne Fuchs	Emergency Management Agency	72 State House Station, 45 Commerce	Augusta, Maine 04333	207-624-4400	https://mema.maryland.gov/Pages/default.aspx
	Acting Director					
Maryland		Emergency Management Agency	Camp Fretterd Military Reservation 5401 Rue Saint Lo Drive	Reisterstown, MD 21136	410-517-3600	www.gov.state.md.us/homelandsecurity.html
	Office of the Executive Director					
Massachusetts	Samantha Phillips	Emergency Management Agency	400 Worcester Road (Route 9 East)	Framingham, MA 01702	508-820-2001	https://www.mass.gov/orgs/massachusetts-emergency-management-agency
	Director					
Michigan	Captain Emmitt McGowan	Michigan State Police	333 S. Grand Avenue	Lansing, Mich. 48909	517-284-3745	https://www.michigan.gov/msp
	Homeland Security Advisor		P.O. 30634			
Minnesota	Joe Kelly	Homeland Security & Emergency Management	445 Minnesota Street, Suite 223	St. Paul, Minn. 55101	651-201-7400	https://dps.mn.gov/divisions/hsem/Pages/default.aspx
	Director					
Mississippi	Jenny Williams	Office of Homeland Security	P.O. Box 958	Jackson, Miss. 39205	601-346-1500	www.homelandsecurity.ms.gov
	Executive Director					

Figure 6.4 List of state homeland security office contacts.

(Continued)

6.2 Challenge of National Policy at the State and Local Levels

Missouri	Kylie Dickneite Director	Office of Homeland Security	P.O. Box 749	Jefferson City, Mo. 65102	573-522-1113	www.dps.mo.gov/homelandsecurity/
Montana		Disaster & Emergency Services	1900 Williams St	Helena, MT 59602	406-324-4777	https://readyandSAFE.mt.gov/
Nebraska	Adjutant General, Major General Daryl Director	Homeland Security	2433 N.W. 24th Street	Lincoln, Neb. 68524-1801	402-471-7421	https://nema.nebraska.gov/preparedness/nebraska-homeland-security
Nevada		Division of Emergency Management - Homeland	2478 Fairview Drive	Carson City, Nev. 89701	775-687-0300	https://dem.nv.gov/Home/DEM_Home/
New Hampshire	Jennifer L. Harper Director	NH Department of Safety Homeland Security and Emergency Management	33 Hazen Drive	Concord, N.H. 03305	603-271-2231	https://www.nh.gov/safety/divisions/hsem/index.html
New Jersey	Jared M. Maples Director	New Jersey Office of Homeland Security and	P.O. Box 091	Trenton, N.J. 08625	609-584-4000	www.njhomelandsecurity.gov
New Mexico		New Mexico Department of Homeland Security & Secretary	P.O. Box 2711	Santa Fe, N.M. 87502	505-476-9600	http://nmdhsem.org
New York		Homeland Security and Emergency Services	1220 Washington Avenue State Office Campus-Building 7A Suite 710	Albany, N.Y. 12242	518-242-5000	http://www.dhss.ny.gov/
North Carolina	Eric A. Hooks Secretary	Department of Public Safety	4201 Mail Service Center	Raleigh, N.C. 27699	919-733-2126	https://www.ncdps.gov/
North Dakota	Cody Schulz Homeland Security Director	Homeland Security Division Department of Emergency Services	P.O. Box 5511	Bismarck, N.D. 58506	701-328-8100	https://www.des.nd.gov/
Ohio	Brian L. Quinn Executive Director	Ohio Homeland Security	1970 W. Broad Street	Columbus, Ohio 43223-1102	614-387-6171	www.homelandsecurity.ohio.gov
Oklahoma	Kim Edd Carter Director	Oklahoma Office of Homeland Security	P.O. Box 11415	Oklahoma City, Okla. 73136-0415	405-425-7296	https://www.ok.gov/homeland/
Oregon	Andrew Phelps Director	Office of Emergency Management	P.O. Box 14370	Salem, Ore. 97309-5062	503-378-2911	https://www.oregon.gov/OEM/Pages/default.aspx
Pennsylvania	Marcus L. Brown Director	Office of Homeland Security	1800 Elmlerton Avenue	Harrisburg, Penn. 17110	717-783-5599	https://www.homelandsecurity.pa.gov/
Rhode Island	Marc R. Pappas Director	Emergency Management Agency	645 New London Ave.	Cranston, R.I. 02920	401-946-9996	http://www.riema.ri.gov/
South Carolina	Kim Stenson Director	Emergency Management Division	2779 Fish Hatchery Road	West Columbia, SC 29172	803-737-8500	https://www.scemd.org/
South Dakota		Office of Homeland Security	118 West Capitol Avenue	Pierre, S.D. 57501	605-773-3450	https://dps.sd.gov/safety-enforcement/homeland-security
Tennessee	Jeff Long Assistant Commissioner	Tennessee Department of Safety and Homeland	312 Rosa L. Parks Avenue	Nashville, TN 37243	615-251-5166	https://www.state.tn.us/safety.html
Texas	Steve McCraw Director	Texas Department of Public Safety	P.O. Box 4087	Austin, Texas 78773-0001	512-424-2000	https://www.dps.texas.gov/
Utah	Jess L. Anderson Commissioner	Department of Public Safety	4501 South 2700 West	Salt Lake City, Utah 84114-1775	801-965-4461	http://publicsafety.utah.gov
Vermont	Captain Kevin Lane Director, Homeland Security	Department of Public Safety	45 State Drive	Waterbury, Vt. 05671-2101	802-241-5000	https://hsu.vermont.gov/
Virginia	Brian Moran Secretary	Public Safety & Homeland Security	PO Box 1475	Richmond, Va. 23218	804-786-5351	https://www.pshs.virginia.gov/
Washington	Robert Ezelle Adjutant General and Director	Washington Military Department Emergency Management Division	20 Aviation Dr. Building 20, MS TA-20	Camp Murray, WA 98430-5112	253-512-8000	http://ml.wa.gov/index.shtml
West Virginia	Thom Kirk Acting Director	Division of Emergency Management	2403 Fairlawn Avenue	Dunbar, West Virginia 25064	304-558-5380	https://emd.wv.gov/Pages/default.aspx
Wisconsin	Adjutant General of the Wisconsin Homeland Security Advisor	Wisconsin Homeland Security	2400 Wright Street PO Box 14587	Madison, Wisc. 53708-8111	608-242-3072	http://hsc.wi.gov/
Wyoming	Lynn Budd Director	Wyoming Office of Homeland Security	5500 Bishop Blvd East Door	Cheyenne, Wyo. 82002	307-777-4900	https://hls.wyo.gov/

Figure 6.4 (CONTINUED) List of state homeland security office contacts.

Homeland Security

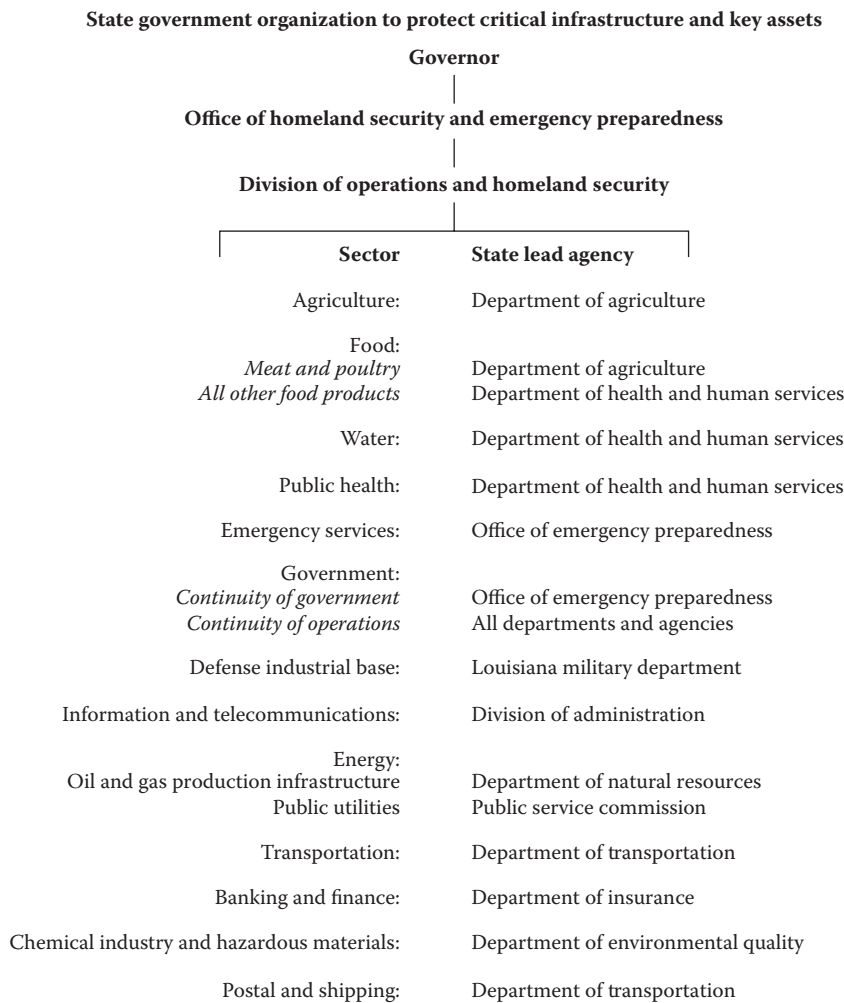


Figure 6.5 Louisiana state homeland security strategy.

All 50 states have some version of an agency dedicated to the task of homeland security. As the states soon discovered, participation at even lower levels, that of the locality, is just as necessary as the federal–state nexus.

6.2.2 Structure at the Local Level

States as large as Texas or Pennsylvania came to realize that local input, local direction, and local assessment are crucial to any plan of homeland security. And in major metropolitan areas, such as New York and Los Angeles, cooperation at the state level is mandatory. What is inevitable is sweeping change in how things have been carried out in traditional law enforcement. Structures changed simply due to the new and corresponding demands. Some argue that the “organizational boundaries” have been changed in ways never envisioned by traditional law enforcement.¹⁴ States such as Pennsylvania divide up their geography into distinct regions (see the map in Figure 6.9).

In each region, the pertinent agencies, for example, the Federal Bureau of Investigation (FBI), Bureau of Alcohol, Tobacco, and Firearms (ATF), Pennsylvania State Police, National Guard,

6.2 Challenge of National Policy at the State and Local Levels

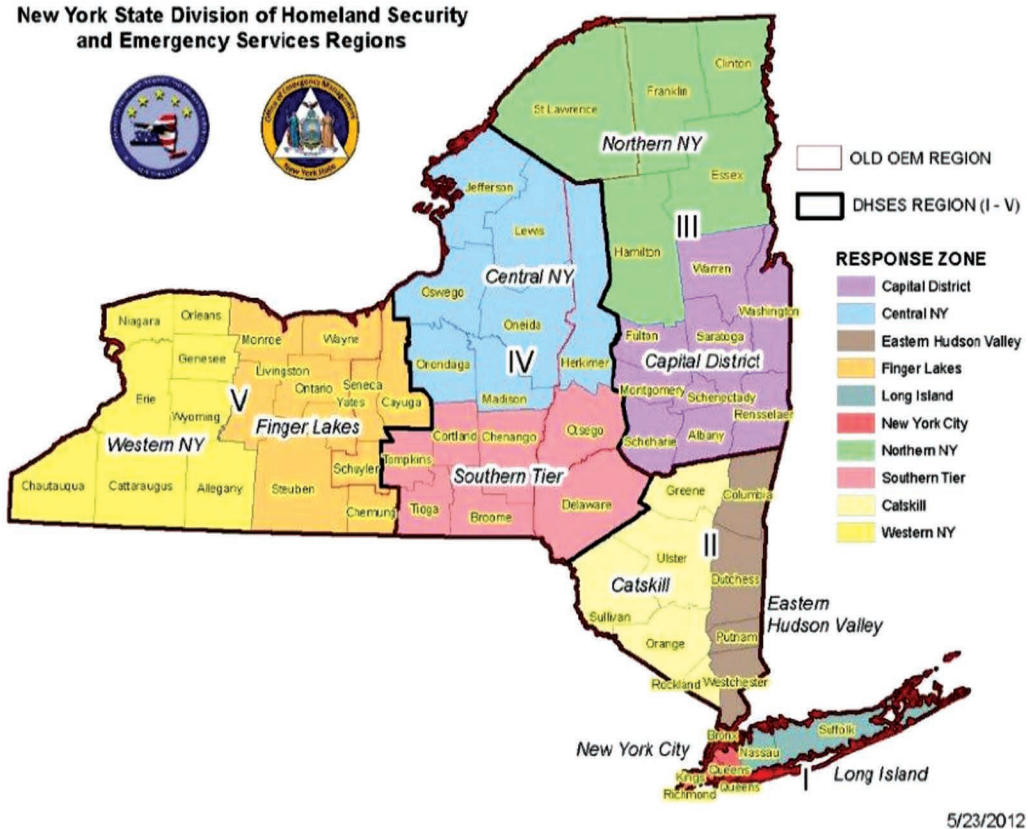


Figure 6.6 New York homeland security and emergency services regions.

Environmental Protection Agency, and health and medical entities, make up its membership. The objectives of the regional program are to

- Develop county task forces
- Develop regional counterterrorism task forces
- Integrate federal/state/county response
- Institutionalize mutual aid in the region
- Establish standing regional response groups
- Encourage regional networking

Another example of state-to-regional design resides in the Commonwealth of Massachusetts. Reporting directly to the statewide Homeland Security Office are five geographically designed regions—the Northeast, Southeast, Central, Western, and Metro Boston—created to support strategic planning and operational coordination at the local level. Regional planning councils are responsible for developing and guiding the implementation of regional homeland security plans. The councils oversee all grant program expenditures. In addition, five regional homeland security advisory councils implement the strategic vision of the state Office of Homeland Security. Collaboration between the regions and the state is now commonplace (see Figure 6.10).

New York State's Homeland Security Goals 2017-2020
Goal 1: Strengthen Intelligence and Information Sharing Capabilities through collaborative partnerships with Federal, State, local, and private sector stakeholders to better protect against and respond to terrorist threats, both foreign and domestic, and other incidents, such as active shooter situations.
Goal 2: Strengthen Counter-Terrorism and Law Enforcement Capabilities by continuing to improve counter-terrorism operations and partnerships across New York State and by building specialized capabilities to address threats and acts of terrorism.
Goal 3: Protect Critical Infrastructure and Key Resources across New York State based on a systematic process of identifying and cataloging infrastructure, conducting site visits and risk assessments, investing in target hardening projects, and providing additional protective and mitigation measures based on the current threat environment.
Goal 4: Enhance Cyber Security Capabilities through outreach and education as well as by implementing programs and policies to identify, prevent, protect against, detect, respond to, and recover from cyber-attacks or other major cyber incidents in collaboration with key partners and stakeholders.
Goal 5: Enhance Citizen and Community Preparedness by better preparing New York State's citizens and communities for disasters and other emergencies, including the ability to sustain themselves for seven to ten days after an event and to assist their neighborhoods in the aftermath of a disaster.
Goal 6: Enhance Emergency Management and Response Capabilities through the implementation of a proactive posture to prepare for and respond to emergencies quickly and effectively.
Goal 7: Strengthen Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) Preparedness and Response Capabilities by acquiring the necessary equipment, training, and resources needed by first responders to effectively detect, interdict, and respond to acts of terrorism or accidents involving CBRNE materials and CBRNE preparedness and response capabilities.
Goal 8: Advance Interoperable and Emergency Communications through the efficient utilization and development of communication resources and procedures to ensure that first responders can effectively communicate with each other during a major incident in order to protect lives and property.
Goal 9: Support Health Emergency Preparedness by readying the State and local communities to distribute medical assistance on a large scale, and supporting the ability of the healthcare community to surge bed capacity and other resources in the event of a large numbers of sick or injured people during any incident.
Goal 10: Become More Resilient against Future Events through resiliency planning and by developing long term recovery capabilities, mitigation initiatives, and other efforts to ensure the continuity of critical systems during a crisis.

Figure 6.7 New York state's stated Homeland Security goals.

6.2.2.1 Fusion Centers

DHS has provided liberal funding sources for the creation of data and information. Fusion Centers in a host of states and increasingly in major metropolitan areas. Fusion Centers are centers for sharing information and intelligence within their jurisdictions, as well as with the federal government.¹⁵ Fusion Centers have now spread across the entire nation—with some being designated “regional” and others “major urban areas.” See Figure 6.11¹⁶ for a national display of the locations.

The crucial dynamic for the Fusion Center is its potentiality for intelligence sharing and dissemination. The fundamental baseline capacities for the Fusion Center must be and are its:

- Ability to receive classified/unclassified information from federal partners
- Ability to assess local implications of threat information through formal risk assessment process
- Ability to further disseminate threat information to other state, local, tribal, and territorial (SLTT) and private-sector entities

6.2 Challenge of National Policy at the State and Local Levels

Table 6.1 State Homeland Security Agency Budgetary Allotments for 2017					
State	Agency Name	FY 2017 Departmental Budget	Total State Budget	Percentage of Total Budget (%)	Ranking
Louisiana	Office of Homeland Security and Emergency Preparedness	\$1,302,175,538.00	\$28,356,600,000.00	4.59214	1
Delaware	Department of Safety and Homeland Security	\$134,025,863.80	\$4,084,051,700.00	3.281689	2
North Dakota	Department of Emergency Services	\$166,065,492.00	\$8,054,000,000.00	2.061901	3
Montana	Disaster and Emergency Services	\$34,584,221.00	\$2,480,172,000.00	1.3944283	4
Indiana	Department of Homeland Security	\$348,807,099.00	\$31,406,000,000.00	1.11064	5
New York	Division of Homeland Security and Emergency Services	\$1,432,506,000.00	\$157,015,269,000.00	0.9123355	6
Connecticut	Emergency Management and Homeland Security	\$174,720,300.00	\$19,807,200,000.00	0.882105	7
Idaho	Office of Emergency Management	\$10,977,000.00	\$3,424,700,100.00	0.57040	8
Florida	Division of Emergency Management	\$331,052,744.00	\$82,154,655,973.00	0.402963	9
Oregon	Office of Emergency Management	\$253,386,817.00	\$74,390,000,000.00	0.351415	10
Washington	Emergency Management Division	\$144,435,984.00	\$46,695,000,000.00	0.309318	11
Wyoming	Office of Homeland Security	\$23,825,665.00	\$7,891,000,000.00	0.30193	12
Alabama	Emergency Management Agency	\$68,098,849.00	\$26,474,000,000.00	0.257229	13
South Dakota	Emergency Services and Homeland Security	\$11,323,153.00	\$4,639,538,438.00	0.244058	14
Vermont	Emergency Management and Homeland Security Division	\$12,567,768.00	\$5,600,000,000.00	0.224424	15
Utah	Emergency Management	\$33,498,600.00	\$15,600,000,000.00	0.214735	16
Mississippi	Office of Homeland Security	\$11,007,306.00	\$5,703,200,000.00	0.1930023	17

(Continued)

Table 6.1 (Continued) State Homeland Security Agency Budgetary Allotments for 2017					
State	Agency Name	FY 2017 Departmental Budget	Total State Budget	Percentage of Total Budget (%)	Ranking
Minnesota	Division of Homeland Security and Emergency Management	\$58,894,000.00	\$38,209,000,000.00	0.1541365	18
Georgia	Homeland Security Division	\$33,309,454.00	\$23,739,270,238.00	0.14031	19
Kansas	Division of Emergency Management	\$20,589,569.00	\$15,528,000,000.00	0.13260	20
Colorado	Division of Homeland Security and Emergency Management	\$32,687,419.00	\$27,149,625,151.00	0.120397	21
New Mexico	Department of Homeland Security and Emergency Management	\$17,850,800.00	\$16,258,511,000.00	0.10979	22
Alaska	Division of Homeland Security and Emergency Management	\$9,445,300.00	\$9,730,700,000.00	0.097067	23
Arkansas	Department of Emergency Management	\$27,905,617.00	\$31,764,694,908.00	0.087851	24
South Carolina	Emergency Management Division	\$20,033,983.00	\$23,074,000,000.00	0.086825	25
Arizona	Department of Homeland Security	\$22,412,900.00	\$40,629,000,000.00	0.055165	26
Rhode Island	Emergency Management Agency	\$4,328,539.00	\$8,964,800,000.00	0.048284	27
Hawaii	Office of Homeland Security	\$6,650,000.00	\$14,110,600,000.00	0.047128	28
Kentucky	Office of Homeland Security	\$5,451,162.00	\$11,413,432,800.00	0.04427	29
Nevada	Division of Emergency Management—Homeland Security	\$4,479,751.00	\$11,527,000,000.00	0.038863	30
North Carolina	Homeland Security	\$8,575,876.00	\$22,174,602,923.00	0.0386743	31
Maine	Emergency Management Agency	\$707,447.00	\$1,867,858,809.00	0.03787	32

(Continued)

6.2 Challenge of National Policy at the State and Local Levels

Table 6.1 (Continued) State Homeland Security Agency Budgetary Allotments for 2017					
State	Agency Name	FY 2017 Departmental Budget	Total State Budget	Percentage of Total Budget (%)	Ranking
New Hampshire	Homeland Security and Emergency Management	\$4,431,070.00	\$11,855,000,000.00	0.03738	33
Nebraska	Emergency Management Agency	\$1,402,870.00	\$ 4,411,690,837.00	0.0317989	34
New Jersey	Office of Homeland Security and Preparedness	\$9,978,000.00	\$34,063,875,000.00	0.0292920	35
Illinois	Emergency Management Agency	\$16,391,500.00	\$55,978,000,000.00	0.02928	36
Michigan	Emergency Management and Homeland Security	\$14,933,800.00	\$55,231,849,400.00	0.0270384	37
California	Homeland Security Division	\$60,159,500.00	\$265,894,000,000.00	0.022625	38
Massachusetts	Homeland Security Division	\$8,573,594.00	\$39,249,262,000.00	0.02184	39
Virginia	Homeland Security Division	\$10,556,500	\$52,186,885,006	0.020228	40
Texas	Division of Emergency Management	\$21,481,000.00	\$144,192,900,000.00	0.01490	41
Maryland	Governor's Office of Homeland Security	\$6,136,500.00	\$42,262,071,879.00	0.01452	42
Tennessee	Homeland Security	\$3,837,700.00	\$33,878,086,600.00	0.0113280	43
Iowa	Homeland Security and Emergency Management	\$2,205,836.00	\$22,694,000,000.00	0.00972	44
Wisconsin	Homeland Security	\$3,962,000.00	\$45,670,000,000.00	0.008675	45
Pennsylvania	Governor's Office of Homeland Security	\$1,920,000.00	\$36,556,400,000.00	0.0052522	46
West Virginia	Division of Homeland Security and Emergency Management	\$2,177,609.00	\$45,670,000,000.00	0.004768	47
Ohio	Homeland Security	\$2,089,997.00	\$64,130,715,702.00	0.0032590	48
Missouri	Office of Homeland Security	–	\$27,322,994,885.00	–	–
Oklahoma	Office of Homeland Security	–	–	–	–

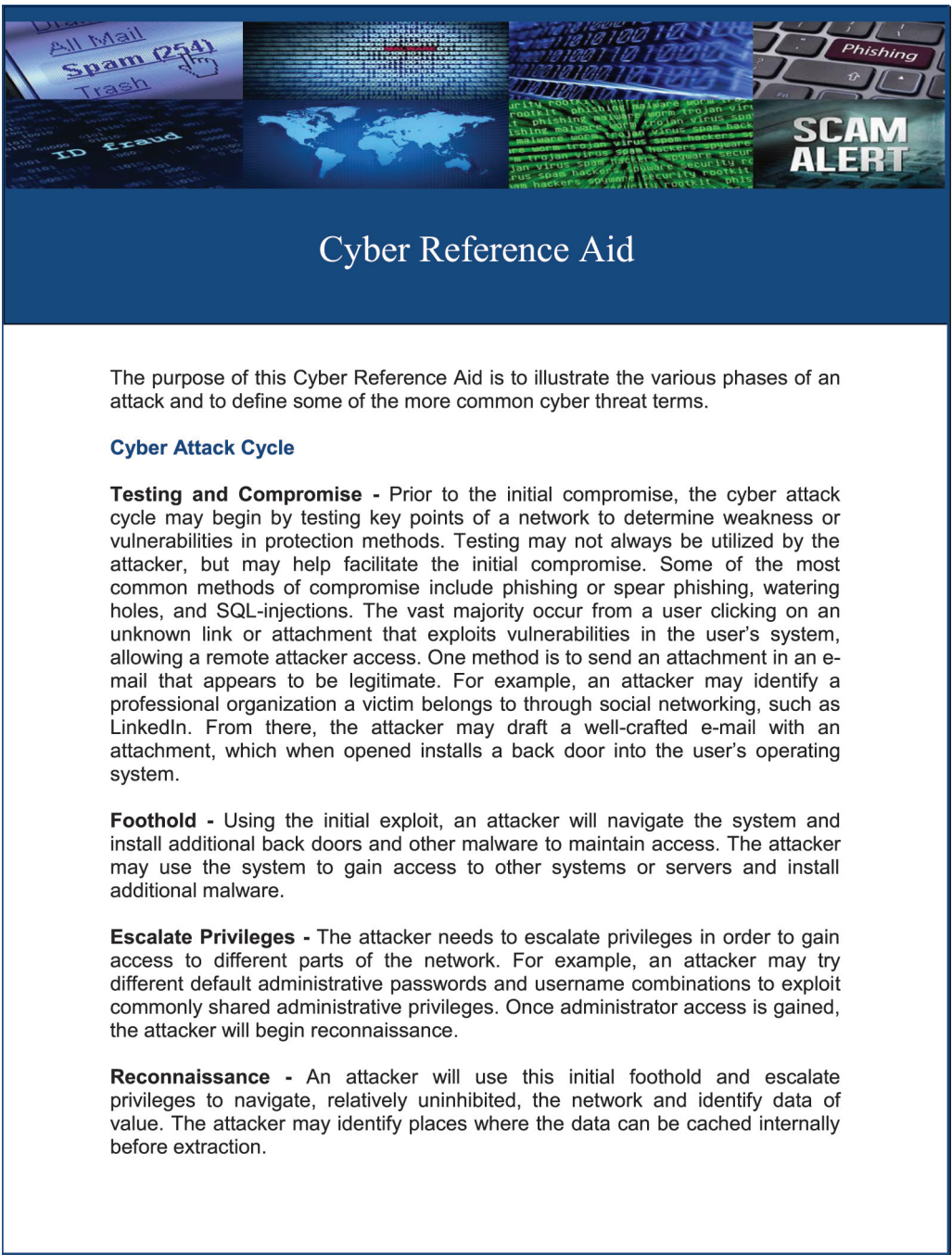


Figure 6.8 Cyber-safety tips.

(Continued)

Extract Data/Take Control - Once the attacker has scouted the network to locate desired data, the attacker will extract the data. This is done by either moving data over to a cached location in or outside the network. The data can be encrypted to avoid being exposed by intrusion detection programs. The data can then be uploaded to a file share or extracted by other means. In addition to extracting data, the attacker may also choose to take control of critical infrastructure components.

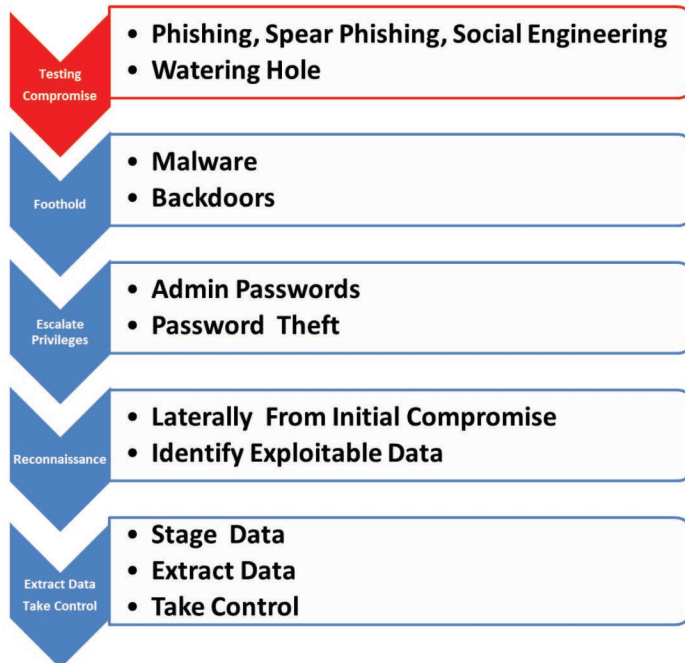


Figure 6.8 (CONTINUED) Cyber-safety tips.

(Continued)

Attacks and Threats Defined

Denial-of-Service Attacks

- **Denial-of-Service (DoS)** - The attacker prevents legitimate users from accessing information or services. DoS attacks most commonly occur when an attacker “floods” a network with requests, thus overwhelming the server, resulting in denial of service.¹
- **Distributed Denial-of-Service (DDoS)** - The attacker gains access to another computer through a security loop-hole to facilitate the attack. The attacker may force the computer, now under their control, to send large amounts of data to a website or send spam to targeted e-mail addresses.²
- **Domain Name Server (DNS) Amplification Attack** - A popular form of DDos in which the attacker uses publically accessible open DNS servers to flood a target system with DNS response traffic. A misconfigured DNS server can be exploited to participate in a DDos attack.³

Social Engineering and Phishing Attacks

- **Phishing Attack** - The attacker uses e-mail or malicious websites to solicit personal information. Attackers often take advantage of current events and certain times of the year.⁴
- **SMiShing** - The attacker uses SMS text messages to “phish” for personally identifiable information and possibly steals funds from the victim. Victims are typically informed that their bank account has been temporarily deactivated, thus requiring them to reply with their credentials to reactivate their account.⁵
- **Social Engineering** - The attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may claim to be a new employee, repair person, or researcher and by asking questions under this persona, may gain enough information to infiltrate an organization’s network.⁶

¹ US-Cert, Understanding Denial-of-Service Attacks, Last Revised February 6, 2013, <http://www.us-cert.gov/ncas/tips/ST04-015>

² US-Cert, Understanding Denial-of-Service Attacks, Last Revised February 6, 2013, <http://www.us-cert.gov/ncas/tips/ST04-015>

³ US-Cert, Alerts and Tips, Last Revised July 22, 2013, <https://www.us-cert.gov/ncas/alerts/TA13-088A>

⁴ US-Cert, Avoiding Social Engineering and Phishing Attacks, Last Revised February 6, 2013, <http://www.us-cert.gov/ncas/tips/ST04-014>

⁵ National Cyber-Forensics & Training Alliance, Phishing Trends, Accessed October 2, 2013, <http://www.ncfta.net/test-post.aspx>

⁶ US-Cert, Avoiding Social Engineering and Phishing Attacks, Last Revised February 6, 2013, <http://www.us-cert.gov/ncas/tips/ST04-014>

Figure 6.8 (CONTINUED) Cyber-safety tips.

(Continued)

- **Spear-Phishing Attack** - The attacker uses a well-crafted e-mail to target select groups of people with something in common. E-mails are presumably sent from organizations or individuals the potential victims would normally get e-mail from, thus making them appear even more legitimate.⁷

Malware

- **Adware** - Adware is a type of malware that allows pop-up ads on computer systems, ultimately taking over a user's Internet browsing.⁸
- **Botnet** - A botnet is a network of private computers, each of which is called a "bot" (short for "robot") infected with malicious software (malware) and controlled as a group without the owners' knowledge for nefarious and, often, criminal purposes. Infected computers are also referred to as "**zombies**."⁹ Botnets are used to conduct a range of activities, to include distributing spam and viruses to conducting DoS attacks.¹⁰
- **Rootkit** - A rootkit is a type of malware that can be installed and hidden without knowledge. Rootkits are not necessarily malicious, but can hide malicious activities. An attacker may install the malicious software by taking advantage of vulnerabilities or facilitating the download through a social engineering attack. Attackers may obtain access to information, monitor actions, modify programs, or perform other functions without detection.¹¹
- **Spyware** - Spyware is a type of malware that exploit infected computers for commercial gain. They can deliver unsolicited pop-up advertisements, steal personal information, monitor web-browsing activity for marketing purposes, or route HTTP requests to advertising sites.¹²
- **Trojan Horse** - A Trojan Horse is a type of malware disguised as legitimate software, often giving an attacker the ability to take remote control over a

⁷ FBI, Spear Phishers, Last Revised February 4, 2009, http://www.fbi.gov/news/stories/2009/april/spearphishing_040109

⁸ National Cyber Security Alliance, StaySafeOnline- Glossary of Terms, Accessed October 2, 2013, <http://staysafeonline.org/stay-safe-online/resources/glossary-of-terms>

⁹ National Cyber Security Alliance, StaySafeOnline- Glossary of Terms, Accessed October 2, 2013, <http://staysafeonline.org/stay-safe-online/resources/glossary-of-terms>

¹⁰ US-Cert, Understanding Hidden Threats: Rootkits and Botnets, Last Revised February 6, 2013, <http://www.us-cert.gov/ncas/tips/ST06-001>

¹¹ US-Cert, Understanding Hidden Threats: Rootkits and Botnets, Last Revised February 6, 2013, <http://www.us-cert.gov/ncas/tips/ST06-001>

¹² McAfee, Glossary, Accessed October 2, 2013, <http://home.mcafee.com/virusinfo/glossary#S>

Figure 6.8 (CONTINUED) Cyber-safety tips.

(Continued)

victim's computer. Unlike viruses and worms, Trojan Horses cannot replicate or propagate themselves.¹³

- **Virus** - A virus is a type of malware designed to spread from computer to computer on its own, potentially damaging the system software by corrupting or erasing data, using available memory, or by altering data. A virus cannot spread without a human action, such as running an infected program.¹⁴
- **Worm** - A worm is a type of malware that can replicate itself over and over within a computer and perform destructive tasks such as using up computer memory resources. Worms do not infect other files as viruses typically do, but instead continue to make copies, resulting in depletion of hard drive space or bandwidth.¹⁵

Other Hidden Threats

- **Back door** - A back door is a feature programmers often build into programs to allow special privileges normally denied to program users. If attackers learn about a back door, the feature may pose a security risk.¹⁶
- **Keylogger** - Keylogging is the action of tracking (or logging) the keys struck on a computer keyboard; usually hidden in the background so users are unaware their actions are being monitored.¹⁷
- **Pharming** - Pharming is when an attacker hijacks a website's domain name, or URL, redirecting users to an imposter website where fraudulent requests for information are made.¹⁸
- **SQL-Injection** - A SQL-injection is the insertion of programming code redirecting the logic of the program, giving control to the attacker.¹⁹

¹³ US-Cert, Understanding Hidden Threats: Rootkits and Botnets, Last Revised February 6, 2013, <http://www.us-cert.gov/ncas/tips/ST06-001>

¹⁴ Norton, Glossary, Accessed October 2, 2013,

http://us.norton.com/security_response/glossary/define.jsp?letter=v&word=virus

¹⁵ Norton, Glossary, Accessed October 2, 2013,

http://us.norton.com/security_response/glossary/define.jsp?letter=w&word=worm

¹⁶ McAfee, Glossary, Accessed October 2, 2013, <http://home.mcafee.com/virusinfo/glossary?ctst=1#B>

¹⁷ National Cyber Security Alliance, StaySafeOnline- Glossary of Terms, Accessed October 2, 2013,

<http://staysafeonline.org/stay-safe-online/resources/glossary-of-terms>

¹⁸ Norton, Internet Security Glossary, Accessed October 1, 2013, http://us.norton.com/security-101/?inid=us_hho_topnav_security_101

¹⁹ Microsoft, SQL Injection, Accessed September 27, 2013, [http://technet.microsoft.com/en-us/library/ms161953\(v=sql.105\).aspx](http://technet.microsoft.com/en-us/library/ms161953(v=sql.105).aspx)

Figure 6.8 (CONTINUED) Cyber-safety tips.

(Continued)

- **Watering Hole** - A watering hole compromise is an unintended download of malicious code (software) that has been injected into legitimate websites the attacker believes will be visited by end users.²⁰

Wireless Threats

Piggybacking – Internet users who fail to secure their wireless network provide opportunity for anyone with a wireless-enabled computer within range of the wireless access point a free ride (piggyback) on their wireless connection. The typical indoor broadcast range of an access point is 150-300 feet. Outdoors, this range may extend as far as 1,000 feet. Piggybacking could present a number of potential problems to include service violations, bandwidth shortages, and abuse by malicious actors.²¹

Wardriving – Wardriving is a specific kind of piggybacking whereby the locations of unsecured wireless networks are located by wardrivers and published online. The information is then available to malicious actors seeking an unsecured connection to mask their identity so they can perpetrate illegal online activity.²²

Resources for Other Cyber Threat Related Terms

- [\[McAfee Glossary\]](#)
- [\[Symantec Glossary\]](#)

²⁰ Trend Micro, Watering Hole 101, Accessed September 27, 2013, <http://about-threats.trendmicro.com/de/webattack/137/Watering+Hole+101>

²¹ US-Cert, Using Wireless Technology Securely, Updated 2008, <http://www.us-cert.gov/sites/default/files/publications/Wireless-Security.pdf>

²² US-Cert, Using Wireless Technology Securely, Updated 2008, <http://www.us-cert.gov/sites/default/files/publications/Wireless-Security.pdf>

Figure 6.8 (CONTINUED) Cyber-safety tips.

Homeland Security

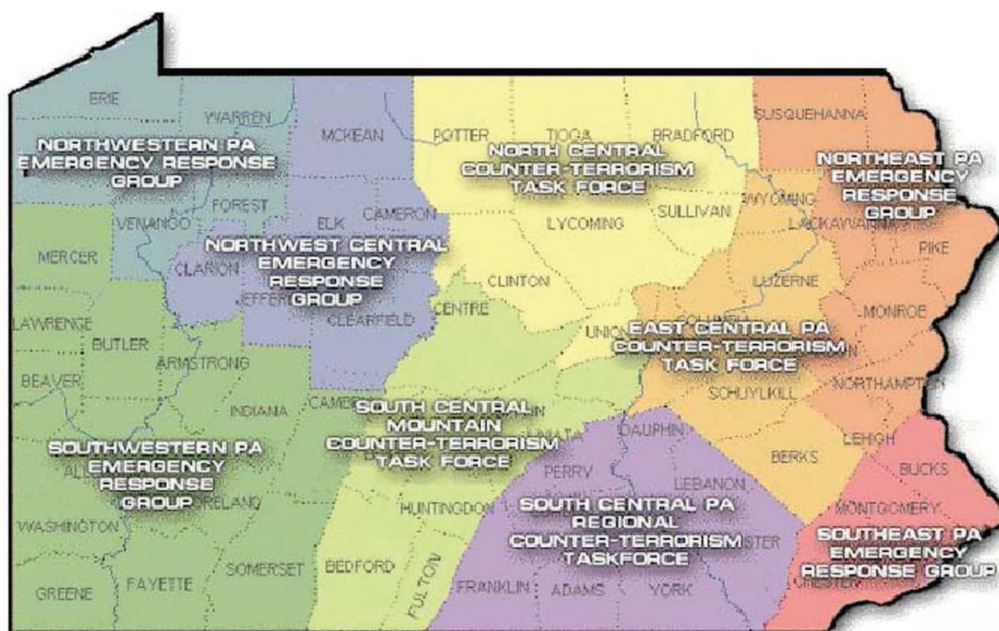


Figure 6.9 Map of Pennsylvania homeland security regions.

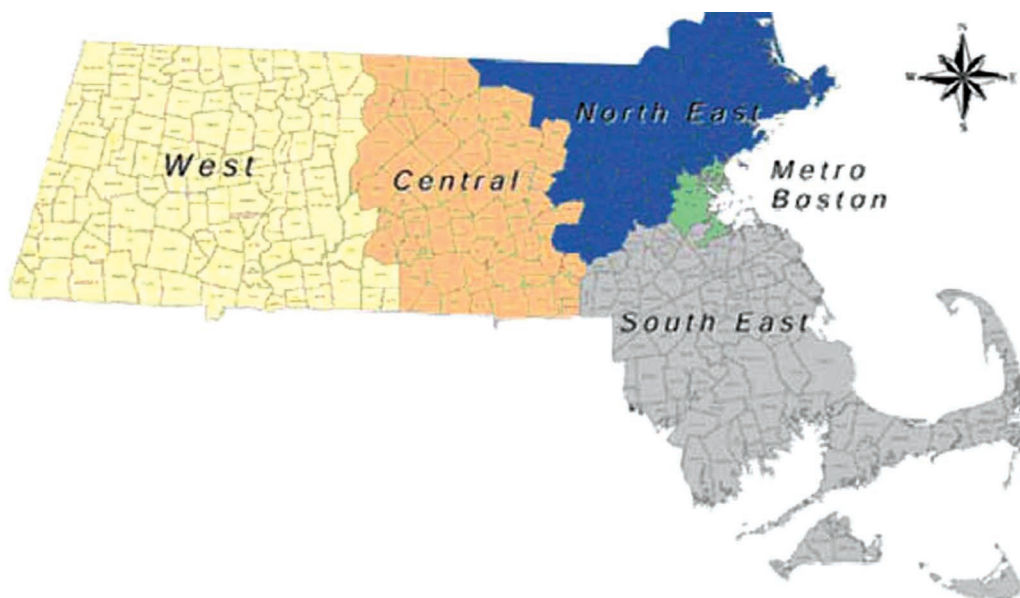


Figure 6.10 Map of Massachusetts homeland security regions.

- Ability to gather locally generated information, aggregate it, analyze it, and share it with federal partners, as appropriate¹⁷

Internet Exercise: Discover much more about the baseline capabilities that every Fusion Center should advance at http://www.dhs.gov/files/programs/gc_1296491960442.shtm.

6.2 Challenge of National Policy at the State and Local Levels

UNCLASSIFIED//FOR OFFICIAL USE ONLY

The National Network

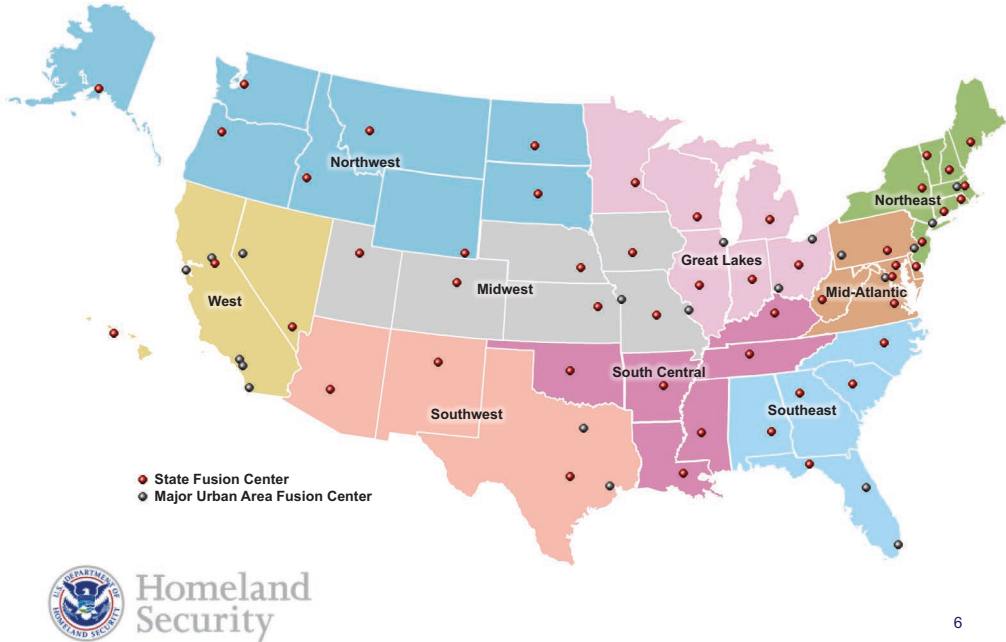


Figure 6.11 Map of Fusion Center locations around the country.

At its core, the Fusion Center must become the locale for a “unified process for reporting, tracking, and accessing”¹⁸ intelligence and information of every variety. The DHS Office of Intelligence and Analysis has now fully integrated a great deal of its intelligence information and data into the operational workings of the Fusion Center. The Office of Intelligence and Analysis collects all relevant information from the governmental agencies that work in support of the nation’s overall mission in homeland defense.¹⁹ Figure 6.12²⁰ shows the interaction.

I&A operates almost like a clearinghouse of information, and our network of Fusion Centers heavily depends on the sharing of this intelligence. The core mission of I&A consists of the following aims:

- Foster a fully synchronized, cohesive enterprise that integrates intelligence into operational functions and drives action through Mission Centers to mitigate all threats to the Homeland, including: counterintelligence, counterterrorism, cyber, economic security, and transnational organized crime.
- Drive multidirectional information exchanges with State, Local, Tribal, and Territorial (SLTT), private sector, and foreign partners to fill critical information and intelligence gaps.
- Produce strategic intelligence products that leverage law enforcement, unique DHS data, and Intelligence Community (IC) holdings to facilitate intelligence-driven decision making by all levels of DHS leadership, other U.S. Government policymakers, and SLTT partners.
- Deliver access to data and systems, infrastructure and analytic expertise, mission readiness services, and Intelligence Community (IC) capabilities to DHS Operational Components.

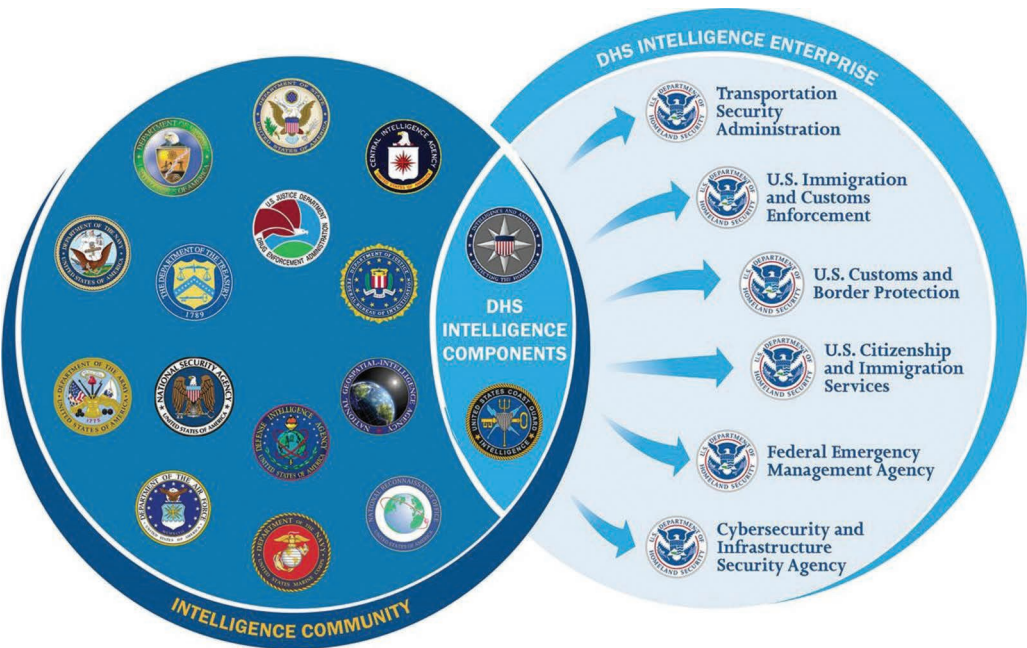


Figure 6.12 Diagram illustrating the U.S. Intelligence Community and how it informs the DHS intelligence enterprise.

- Ensure unique DHS datasets are available to Mission Centers, the IC, and law enforcement partners to bolster collaborative government efforts to counter threats.
- Provide unique data on immigration, travel and intelligence, analytic tools, and technical infrastructure to assist the U.S. Government stand-up of the National Vetting Center.
- Invest in our people, who are critical for achieving the above operating principles, by continuously enhancing our talent and leadership development to foster a cadre of high-performing Homeland Security intelligence professionals.²¹

Every state now has a Fusion Center.²² In addition, major urban or regional areas such as Orange County, California, and Boston Regional, to name two, have erected Centers.²³ See Table 6.2.²⁴ State Fusion Centers are primarily of two designs:

- *Primary fusion centers:* A primary fusion center typically provides information sharing and analysis for an entire state. These centers are the highest priority for the allocation of available federal resources, including the deployment of personnel and connectivity with federal data systems.
- *Recognized fusion centers:* A recognized fusion center typically provides information sharing and analysis for a major urban area. As the Federal Government respects the authority of state governments to designate fusion centers, any designated fusion center not designated as a primary fusion center is referred to as a recognized fusion center.²⁵

Major cities and urban areas have constructed what DHS calls *Recognized Fusion Centers*, the most recent listing including, as of July 2017:

- Austin Regional Intelligence Center, Austin, Texas
- Boston Regional Intelligence Center, Boston, Massachusetts

6.2 Challenge of National Policy at the State and Local Levels

Table 6.2 Listing of State Fusion Centers					
State	Name of Fusion Center	Mailing Address	Physical Address	Phone Number	Email
Alabama	Alabama Fusion Center	Post Office Box 1511 Montgomery, AL 36102	201 S Union St Montgomery, AL 36104	(334) 517-2660	fusioncenter@afc.alacop.gov
Alaska	Alaska Information and Analysis Center (AKIAC)	101 East Sixth Avenue Anchorage, AK 99501	101 East Sixth Avenue Anchorage, AK 99501	(907) 265-8123	akiac@alaska.gov
Arizona	Arizona Counter Terrorism Information Center (ACTIC)	Post Office Box 6638 Phoenix, AZ 85005	16212 N 28th Ave Phoenix, AZ 85053	(877) 272-8329	actic@azdps.gov
Arkansas	Arkansas State Fusion Center	1 State Police Plaza Drive Little Rock, AR 72209	1 State Police Plaza Drive Little Rock, AR 72209		arfusioncenter@asp.arkansas.gov
California	Orange County Intelligence Assessment Center	2644 Santiago Canyon Road Silverado, CA 92676-9791	2644 Santiago Canyon Road Silverado, CA 92676-9791	(714) 628-3024	ociac@ocsd.org
California	Los Angeles Joint Regional Intelligence Center (LAJRIC)	12440 East Imperial Highway Norwalk, CA 90650	12440 East Imperial Highway Norwalk, CA 90650	(562) 345-1100	jric@lajric.gov
California	Northern California Regional Intelligence Center (NCRIC)	P.O. Box 36102 San Francisco, CA 94102	450 Golden Gate Ave., 14th Floor San Francisco, CA 94102	(866) 367-8847	dutyofficer@ncric.org
California	Central California Intelligence Center/ Sacramento Regional Terrorism Threat Assessment Center		3720 Dudley Blvd. McClellan, CA 95652	(888) 884-8383	sacrttac@sacsheriff.com
California	State Terror Threat Assessment Center	Post Office Box 944255 Sacramento, CA 94244	3741 Bleckley St. Mather, CA 95655	(916) 227-1280	ohsdutyanalyst@ohs.ca.gov

(Continued)

Table 6.2 (Continued) Listing of State Fusion Centers					
State	Name of Fusion Center	Mailing Address	Physical Address	Phone Number	Email
California	San Diego Law Enforcement Coordination Center (SD-LECC)		4181 Ruffin Road San Diego, CA 92123	(858) 495-7200	rttac@sdrttac.org
Colorado	Colorado Information Analysis Center	690 Kipling Street Lakewood, CO 80215	690 Kipling Street Lakewood, CO 80215	(877) 509-2422	ciac@ciac.co.gov
Connecticut	Connecticut Intelligence Center (CTIC)	600 State Street New Haven, CT 06511	600 State Street New Haven, CT 06511	(203) 777-6311	ctic@nespin.riss.net
Delaware	Delaware Information Analysis Center	Post Office Box 430 Dover, DE 19904	1575 McKee Rd. Dover, DE 19904	(302) 739-5996	diac@state.de.us
District of Columbia	Washington Regional Threat and Analysis Center	2720 Martin Luther King, Jr. Avenue, S.E., Washington, D.C. 20032	300 Indiana Ave NW Washington, DC 20001	(202) 481-3007	wrtac@dc.gov
Florida	Florida Fusion Center	P.O. Box 1489 Tallahassee, FL 32302	2331 Phillips Road Tallahassee, FL 32308	(850) 410-7645	floridafusioncenter@fdle.state.fl.us
Florida	Miami Dade Fusion Center		11200 NW 20th St Doral, FL 33172	(305) 470-3880	ioc@mdpd.com
Florida	Central Florida Intelligence Exchange (CFIX)	PO Box 608423 Orlando, Florida 32860	6643 Hazeltine National Drive Orlando, FL 32860		ctic@fdle.state.fl.us
Georgia	Georgia Information Sharing and Analysis Center (GISAC)	Post Office Box 29649 Atlanta, GA 30359	2635 Century Parkway, N.E. Atlanta, GA 39345	(404) 486-6420	generalinfo@gisac.gbi.ga.gov
Hawaii	Pacific Regional Information Clearinghouse	500 Ala Moana Blvd. Honolulu, HI 96813	500 Ala Moana Blvd. Honolulu, HI 96813	(800) 952-5258	pacclear@hi.hidta.net

(Continued)

6.2 Challenge of National Policy at the State and Local Levels

Table 6.2 (Continued) Listing of State Fusion Centers					
State	Name of Fusion Center	Mailing Address	Physical Address	Phone Number	Email
Idaho	Idaho Criminal Intelligence Center	700 S Stratford Dr, Meridian, Ada, Idaho 83642	700 S Stratford Dr, Meridian, Ada, Idaho 83642	(208) 846-7676	icic@fusion.idaho.gov
Illinois	Statewide Terrorism and Intelligence Center (STIC)	2100 S. Dirksen Parkway Springfield, IL 62703	2100 S. Dirksen Parkway Springfield, IL 62703	(877) 455-7842	stic@isp.state.il.us
Indiana	Indiana Intelligence Fusion Center	302 W. Washington Street Room E243 Indianapolis, IN 46204	302 W. Washington Street Room E243 Indianapolis, IN 46204	(866) 400-4432	iifc@iifc.in.gov
Iowa	Iowa Fusion Center	215 East 7th Street Des Moines, Iowa 50319	215 East 7th Street Des Moines, Iowa 50319	(800) 308-5983	inthsin@dps.state.ia.us
Kansas	Kansas Threat Integration Center (KSTIC)	2722 Southwest Topeka Blvd Topeka, KS 66611	2722 Southwest Topeka Blvd Topeka, KS 66611	(785) 2741503	kstic@tag.ks.gov
Kentucky	Kentucky Fusion Center	Post Office Box 1757 Frankfort, KY 40602	200 Mero St Frankfort, KY 40622	(502) 564-2081	fusioncenter@ky.gov
Louisiana	Louisiana State Analytical and Fusion Exchange (LA-SAFE)	376A East Airport, Baton Rouge, LA 70806	376A East Airport, Baton Rouge, LA 70806	(225) 925-1978	lafusion.center@dps.la.gov
Maine	Maine Intelligence Analysis Center	45 Commerce Drive, Suite 1 Augusta, ME 04330	164 State House Station Augusta, ME 04330	(207) 624-7280	miaac@nespin.riss.net
Maryland	Maryland Coordination and Analysis Center (MCAC)		7125 Ambassador Road Woodlawn, MD 21244	(800) 492-8477	mdwatch@leo.gov

(Continued)

Table 6.2 (Continued) Listing of State Fusion Centers					
State	Name of Fusion Center	Mailing Address	Physical Address	Phone Number	Email
Massachusetts	Boston Regional Intelligence Center (BRIC)		One Schroeder Plaza Roxbury, MA 2120	(617) 353-4328	bric.bpd@ci.boston.ma.us
Massachusetts	Commonwealth Fusion Center	124 Acton Street, 2nd Floor Maynard, MA 01754	124 Acton Street, 2nd Floor Maynard, MA 01754	(978) 451-3700	fusion@pol.state.ma.us
Michigan	Michigan Intelligence Operations Center		714 S. Harrison Road East Lansing, MI 48823	(877) 616-4677	mioc@michigan.gov
Michigan	Detroit Southeast Michigan Information and Intelligence Center		28 Adams Ave E Detroit, MI 48226	(313) 976-4625	
Minnesota	Minnesota Joint Analytical Center		Suite 820 111 Washington Avenue South Minneapolis, MN 55401	(612) 373-2840	info@icefishx.org
Mississippi	Mississippi Analysis and Information Center	1 MEMA Drive Pearl, MS 39208	1 MEMA Drive Pearl, MS 39208	(601) 933-7200	msaic@mdps.state.ms.us
Missouri	KC Regional TEW	635 Woodland Ave., Suite 2105B Kansas City, MO 64106	635 Woodland Ave., Suite 2105B Kansas City, MO 64106	(816) 889-6130	KCTEW@kcpd.org
Missouri	Missouri Information Analysis Center		2302 Militia Drive Jefferson City, MO 65101	(866) 362-6422	miac@mshp.dps.mo.gov
Missouri	St. Louis Terrorism Early Warning Group		7900 Forsyth Blvd St. Louis, MO 63105	(314) 615-4839	info@sltew.org
Montana	Montana All-Threat Intelligence Center (MATIC)	Post Office Box 4789 Ft. Harrison, MT 59636	2225 11th Ave Helena, MT 59601	(406) 444-1330	dojintel@mt.gov

(Continued)

6.2 Challenge of National Policy at the State and Local Levels

Table 6.2 (Continued) Listing of State Fusion Centers					
State	Name of Fusion Center	Mailing Address	Physical Address	Phone Number	Email
Nebraska	Nebraska Information Analysis Center		3800 NW 12th St Lincoln, NE 68521	(402) 479-4099	nefusioncenter@nebraska.gov
Nevada	Nevada Threat Analysis Center	555 Wright Way Carson City, NV 89711	2478 Fairview Drive Carson City, NV 89701	(775) 687-0450	ntac@dps.state.nv.us
Nevada	Southern Nevada Counter-Terrorism Center	6767 Spencer Street, Las Vegas Nevada 89119	6767 Spencer Street, Las Vegas Nevada	(702) 828-2200	doc@lvmpd.com
New Hampshire	New Hampshire Information and Analysis Center		110 Smokey Bear Blvd Concord, NH 03305	(603) 271-0300	NhspIntel@dos.nh.gov
New Jersey	New Jersey Regional Operations Intelligence Center	Post Office Box 7068 West Trenton, NJ 08628-0068	2 Schwarzkopf Drive West Trenton, NJ 08628	(866) 472-3365	roic@gw.njsp.org
New Mexico	New Mexico All Source Intelligence Center (NMAISIC)	PO Box 27111 87502	13 Bataan Blvd., Santa Fe, NM 87504	(505) 476-9600	intelligence.fusion@state.nm.us
New York	New York State Intelligence Center	630 Columbia Street Extension Latham, NY 12110	630 Columbia Street Extension Latham, NY 12110	(866) 723-3697	ciu@nysic.ny.gov
North Carolina	North Carolina Information Sharing and Analysis Center		310 New Bern Ave. Raleigh, NC 27601	(888) 624-7222	ncisaac@ncdoj.gov
North Dakota	North Dakota State and Local Intelligence Center		400 Fraine Barracks Rd Bismarck, ND 58506	(866) 885-8295	ndslc@nd.gov

(Continued)

Table 6.2 (Continued) Listing of State Fusion Centers

State	Name of Fusion Center	Mailing Address	Physical Address	Phone Number	Email
Ohio	Cincinnati/Hamilton Regional Terrorism Early Warning Group		2000 Radcliff Drive Cincinnati, OH 45204	(513) 263-8000	saic@dps.state.oh.us
Ohio	Strategic Analysis and Information Center	2855 West Dublin Grandville Road Columbus, OH 43235	2855 West Dublin Grandville Road Columbus, OH 43235	(614) 799-3555	saic@dps.state.oh.us
Oklahoma	Oklahoma Information Fusion Center	6600 N Harvey Oklahoma City, OK 73116	6600 N Harvey Oklahoma City, OK 73116	(405) 848-6724	fusion@osbi.ok.gov
Oregon	Terrorism Fusion Center (TITAN)	610 Hawthorne Ave., Suite 210 Salem, OR 97301	610 Hawthorne Ave., Suite 210 Salem, OR 97301	(503) 378-6347	oregonfusioncenter@doj.state.or.us
Pennsylvania	Pennsylvania Criminal Intelligence Center (PaCIC)	1800 Elmerton Avenue Harrisburg, PA 17110	1800 Elmerton Avenue Harrisburg, PA 17110		sp-intelligence@state.pa.us
Rhode Island	Rhode Island State Fusion Center		10 Dorrance St Providence, RI 02903	(866) 490-8477	fusion@risp.dps.ri.gov
South Carolina	South Carolina Intelligence and Information Center		1731 Bush River Road, Columbia, SC 29210	(866) 472-8477	scic@sled.sc.gov
South Dakota	South Dakota Fusion Center		1302 US 14 Pierre, SD 57501	(605) 773-3178	sdfusioncenter@state.sd.us
Tennessee	Tennessee Regional Information Center		901 R.S. Gass Boulevard Nashville, TN 37243	(877) 250-2333	tfc@tn.gov
Texas	Houston Regional Intelligence Service Center		5320N. Shepherd Drive Houston, TX 77091	(713) 884-4710	cidcdu@leo.gov

(Continued)

6.2 Challenge of National Policy at the State and Local Levels

Table 6.2 (Continued) Listing of State Fusion Centers					
State	Name of Fusion Center	Mailing Address	Physical Address	Phone Number	Email
Texas	North Central Texas Fusion Center	4300 Community Avenue McKinney, TX 75071	4300 Community Avenue McKinney, TX 75071	(972) 548-5537	homelandsecurity@co.collin.tx.us
Texas	Texas Intelligence Center		5805 N. Lamar Blvd. Austin, TX 78752	(866) 786-5972	txdpsintelcenter@txdps.state.tx.us
Utah	Statewide Information & Analysis Center (SIAC)	410 West 9800 South, Suite 370 Sandy, Utah 84070	410 West 9800 South, Suite 370 Sandy, Utah 84070	(801) 256-2360	saic@utah.gov
Vermont	Vermont Fusion Center	188 Harvest Lane Williston, VT 09405	188 Harvest Lane Williston, VT 09405	(802) 872-6110	vtfusion@dps.state.vt.us
Virginia	National Capital Region Intelligence Center		4100 Chain Bridge Road Fairfax, VA 22030	(703) 212-4590	fcpd-ncric@fairfaxcounty.gov
Virginia	Virginia Fusion Center		7700 Midlothian Turnpike Richmond, VA 23235	(804) 674-2196	vfc@vsp.virginia.gov
Washington	Washington State Fusion Center (WSFC)	Post Office Box 42600 Olympia, WA 98504	1110 Third Ave, Seattle, WA 98101	(877) 843-9522	wafusion@wsp.wa.gov
Wisconsin	Southeastern Wisconsin Terrorism Alert Center		749 West State St Milwaukee, WI 53233	(414) 935-7767	ifc@milwaukee.gov
Wisconsin	Wisconsin Statewide Intelligence Center	Post Office Box 7857 Madison, WI 53707-7857	2445 Darwin Rd Madison, WI 53703	(608) 242-5393	wsic@doj.state.wi.us
Wyoming	Wyoming Criminal Intelligence Center		316 West 22 Street Cheyenne, WY 82002	(307) 777-7181	klandm@dc.i.wyo.gov

Homeland Security

- Central California Intelligence Center, Sacramento, California
- Central Florida Intelligence Exchange, Orlando, Florida
- Chicago Crime Prevention and Information Center, Chicago, Illinois
- Cincinnati/Hamilton County Regional Terrorism Early Warning Group, Cincinnati, Ohio
- Dallas Fusion Center, Dallas, Texas
- Delaware Valley Intelligence Center, Philadelphia, Pennsylvania
- Detroit and Southeast Michigan Information and Intelligence Center, Detroit, Michigan
- El Paso Multi-Agency Tactical Response Information eXchange (MATRIX), El Paso, Texas
- Houston Regional Intelligence Service Center, Houston, Texas
- Kansas City Terrorism Early Warning Fusion Center, Kansas City, Missouri
- Los Angeles Joint Regional Intelligence Center, Los Angeles, California
- Nevada Threat Analysis Center, Carson City, Nevada
- North Central Texas Fusion Center, McKinney, Texas
- Northeast Ohio Regional Fusion Center, Cleveland, Ohio
- Northern California Regional Intelligence Center, San Francisco, California
- Northern Virginia Regional Intelligence Center, Fairfax, Virginia
- Orange County Intelligence Assessment Center, Orange County, California
- San Diego Law Enforcement Coordination Center, San Diego, California
- Southeast Florida Fusion Center, Miami, Florida
- Southeastern Wisconsin Threat Analysis Center, Milwaukee, Wisconsin
- Southwest Texas Fusion Center, San Antonio, Texas
- Southwestern PA Region 13 Fusion Center, Pittsburgh, Pennsylvania
- St. Louis Fusion Center, St. Louis, Missouri

DHS's Office of Intelligence and Analysis provides personnel with operational and intelligence skills to staff the Fusion Centers. The Centers serve many purposes including:

- Help classified and unclassified information flow
- Provide expertise
- Coordinate with local law enforcement and other agencies
- Provide local awareness and access (see Figure 6.13)

The I&A Office has deployed intelligence officers to state fusion centers in

- Arizona
- California
- Colorado
- Connecticut
- Georgia

6.2 Challenge of National Policy at the State and Local Levels

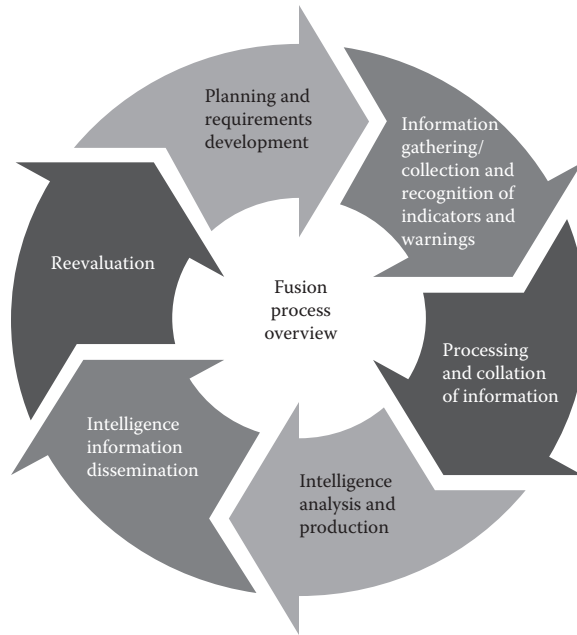


Figure 6.13 Figure from the U.S. government's information sharing environment depicting the fusion process as a continuous cycle in which inputs from various sources are brought together to provide state and local context to help enhance the national threat picture. Available at <https://www.ise.gov/national-network-state-and-major-urban-area-fusion-centers>.

- Florida
- Illinois
- Indiana
- Louisiana
- Maryland
- Massachusetts
- New Jersey
- New York
- Ohio
- South Carolina
- Virginia
- Washington

Internet Exercise: Find out about the many facets of the Fusion Center at https://www.dhs.gov/sites/default/files/publications/Fusion%20Centers%20Handout_0.pdf

6.2.3 Funding and Local Initiatives

The funding and grant systems for DHS recognize the fundamental decentralization of local and state homeland security efforts. The Homeland Security Grant program funds planning, organization, equipment, training, and exercise activities in support of the National Preparedness

Homeland Security

Guidelines, as well as the National Incident Management System (NIMS), the National Response Framework (NRF), and the National Infrastructure Protection Plan (NIPP). The funds are sent directly to states for specific programs and purposes, including planning, equipment, training, and exercise activities, as well as for the implementation of new programs and initiatives. DHS additionally earmarks funds for four other sectors essential to homeland security:

Urban Area Security Initiative (UASI) Grant Program funds address the unique multidisciplinary planning, operations, equipment, training, and exercise needs of high-threat, high-density urban areas.

Law Enforcement Terrorism Prevention Program (LETPP) focuses on the prevention of terrorist attacks and provides law enforcement and public safety communities with funds to support the following activities: intelligence gathering and information sharing through enhancing/establishing fusion centers; hardening high-value targets; planning strategically; continuing to build interoperable communications; and collaborating with non-law-enforcement partners, other government agencies, and the private sector.

Public Safety Interoperable Communications (PSIC) Grant Program assists public safety agencies in the acquisition of, deployment of, or training for the use of interoperable communications systems that can utilize a reallocated public safety spectrum in the 700 MHz band for radio communication.

Infrastructure Protection Program (IPP) supports specific activities to protect critical infrastructure, such as ports, mass transit, highways, rail, and transportation. IPP grants fund a range of preparedness activities, including strengthening infrastructure against explosive attacks, preparedness planning, equipment purchase, training, exercises, and security management and administration costs. IPP comprises five separate grant programs: Transit Security, Port Security, Buffer Zone Protection, Trucking Security, and Intercity Bus Security.

For the funding cycle 2020, DHS has shifted these priorities a bit with a new emphasis which includes:

- Cybersecurity
- Soft targets and crowded places
- intelligence and information sharing
- emerging threats.

Moreover, DHS, by and through the Federal Emergency Management Agency (FEMA), erects Citizen Corps Councils in nearly 2,500 communities across the United States. Citizen Corps, coordinated by DHS, focuses on opportunities for people across the country to participate in a range of measures to make their families, homes, and communities safer from the threats of terrorism, crime, and disasters of all kinds. Citizen Corps also brings together a community's first responders, CERT teams, firefighters, emergency health-care providers, law enforcement, and emergency managers with its volunteer resources.²⁶

Internet Exercise: See how CERT teams and Citizen Corps could mutually assist and complement one another at <https://www.ready.gov/collection/cert-registration-system-presentation>

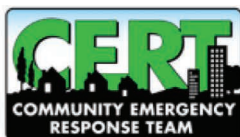
Citizen Corps will help people across America take a more active role in crime prevention, support the emergency medical community, and be better trained in a wide range of emergency preparedness and disaster response activities (see Figure 6.14).

The focus of Citizen Corps work is at the local level. The scope of the Citizen Corps covers a wide range of activities. Citizen Corps Councils help drive local citizen participation by coordinating Citizen Corps programs, developing community action plans, assessing possible threats, and identifying local resources. Examples of corps programs are shown in Figure 6.15.

6.2 Challenge of National Policy at the State and Local Levels



Figure 6.14 Citizen Corps logo.



The Community Emergency Response Team (CERT) Program educates people about disaster preparedness and trains them in basic disaster response skills, such as fire safety, light search and rescue, and disaster medical operations. Using their training, CERT members can assist others in their neighborhood or workplace following an event and can take a more active role in preparing their community. The program is administered by the Federal Emergency Management Agency.



The Fire Corps promotes the use of citizen advocates to enhance the capacity of resource-constrained fire and rescue departments at all levels: volunteer, combination, and career. Citizen advocates can assist local fire departments in a range of activities including fire safety outreach, youth programs, and administrative support. Fire Corps provides resources to assist fire and rescue departments in creating opportunities for citizen advocates and promotes citizen participation. Fire Corps is funded through DHS and is managed and implemented through a partnership between the National Volunteer Fire Council, the International Association of Fire Fighters, and the International Association of Fire Chiefs.



The National Neighborhood Watch Program (formerly USAonWatch), housed within the National Sheriffs' Association, has worked to unite law enforcement agencies, private organizations, and individual citizens in a nation-wide effort to reduce crime and improve local communities. In the aftermath of September 11, 2001, Neighborhood Watch programs have expanded beyond their traditional crime prevention role to help neighborhoods focus on disaster preparedness, emergency response and terrorism awareness. The Neighborhood Watch Program draws upon the compassion of average citizens, asking them to lend their neighbors a hand.



The Medical Reserve Corps (MRC) Program strengthens communities by helping medical, public health and other volunteers offer their expertise throughout the year as well as during local emergencies and other times of community need. MRC volunteers work in coordination with existing local emergency response programs and also supplement existing community public health initiatives, such as outreach and prevention, immunization programs, blood drives, case management, care planning, and other efforts. The MRC program is administered by HHS.



Volunteers in Police Service (VIPS) works to enhance the capacity of state and local law enforcement to utilize volunteers. VIPS serves as a gateway to resources and information for and about law enforcement volunteer programs. Funded by DOJ, VIPS is managed and implemented by the International Association of Chiefs of Police.



Citizen Corps is coordinated nationally by the Department of Homeland Security. DHS also works closely with the Corporation for National and Community Service (CNCS) to promote volunteer service activities that support homeland security and community safety. CNCS is a federal agency that operates nationwide service programs such as AmeriCorps, Senior Corps, and Learn and Serve America. Participants in these programs may support Citizen Corps Council activities by helping to establish training and information delivery systems for neighborhoods, schools, and businesses, and by helping with family preparedness and crime prevention initiatives in a community or across a region. .

Figure 6.15 An assortment of Citizen Corps programs.

Homeland Security

Internet Exercise: Review the many organizations and associations involved in Citizen Corps at <https://www.ready.gov/citizen-corps-partner-programs>.

6.3 Fine Line of National Defense and Homeland Security

It is unlikely that any firm line can be drawn between the worlds of national and homeland security. At one time, this may have been possible. Given the events of 9/11, the interconnectedness and integration of the military/defense function with that of law enforcement and security became grotesquely obvious. Indeed, the terrorists seemed to have deduced this by their mixture of targets, from the attempted White House attack, to the Twin Towers and the distressing crash into the Pentagon (Figure 6.16).

In a way, it is absurd to think that these dual lines of defense do not merge in many sectors. Some might even argue that the Iraq and Afghanistan campaigns are extensions of a security and police effort to track down the perpetrators of terror. The argument has both appeal and merit. That there must be some sort of collaboration between the military complex and the arm of homeland security is now standard operating procedure.

When speaking of the military, we reference the historic four major branches of the service. The U.S. Coast Guard (USCG) has long been out of the Department of Defense (DoD) province, initially being in the U.S. Treasury Department, while today it is housed in DHS. Hence, the mindset of the USCG has always been in hazard and human tragedy. So too the continuous contribution of the National Guard—an agency that attends to human suffering with professionalism and skill. Shortly after the attack of 9/11, the remaining arms of the military swung into action. The entire structure of the military was reorganized into a unified command as outlined in Figure 6.17.²⁷

Five zones are apportioned the responsibility for defense against terror based on the designated geography:

U.S. Northern Command (USNORTHCOM)

U.S. Southern Command (USSOUTHCOM)

U.S. Pacific Command (USPACOM)

U.S. European Command (USEUCOM)

U.S. Central Command (USCENTCOM)



Figure 6.16 The Pentagon on 9/11.

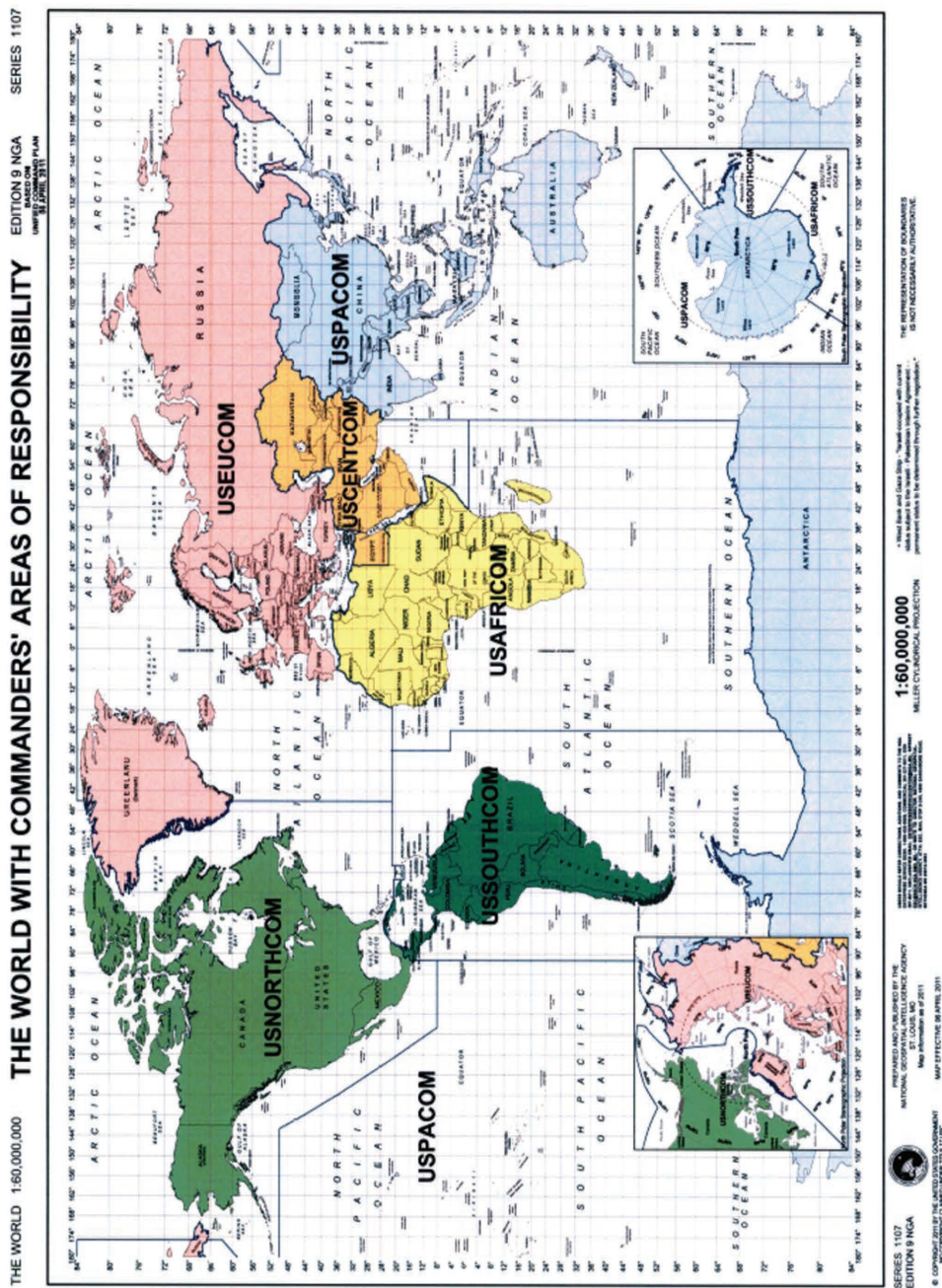


Figure 6.17 A world map and explanation of military commanders' areas of responsibility.

Homeland Security



Figure 6.18 Air National Guard over New York City area.



Figure 6.19 The logos for the various military commands.

The reorientation of the military into a terror mentality has been nothing short of dramatic, but the events of 9/11 prompted the re-examination. To be sure, Americans are generally reticent about military authority, and only in cases of extreme national emergency are the armed forces called on to assist. It could be argued that part of Katrina’s problem related to this hesitancy. As we gazed at the television sets, how many of us wondered aloud, “Where is the military assistance?” By any measure, it was slow in coming (Figure 6.18).

The military-defense complex further categorizes 11 distinct Combatant commands which are tied to geographic areas and the subject matter of those commands. In 2019, the increase in commands reflected new orientations and emphases such as the Space Command and Cyber Command. Figure 6.19²⁸ portrays the command by its respective symbol.

All these steps lead to better unification and shared responsibility in the defense of the homeland. The utilization of drones manifests how close the homeland and military world

6.3 Fine Line of National Defense and Homeland Security



Figure 6.20 Florida National Guard Soldiers from the 2–124 Infantry Regiment are performing missions in the nation’s capital to protect national monuments and ensure citizens’ right to peaceful assembly. The Florida National Guard members assigned to these missions are specially trained to assist law enforcement authorities in protecting life and preserving property, peace, and public safety. (Photo by Sgt. Leia Tascarini.)

interest. Of present interest has been the often-contentious debate about using military personnel in civil disturbance, riot and looting situations witnessed in the early summer of 2020. While military command should not be relied upon to regulate or oversee the normal, peaceful protest of those engaging in free expression and speech—there have been times in American history where the military were correctly relied upon to minimize violent civil unrest and looting. During 1992 the Rodney King incident prompted severe unrest in Los Angeles while in the District of Columbia, just as in the summer of 2020, monuments and national historic locations were allegedly vandalized by protestors enraged by the wrongful death of George Floyd. See Figure 6.20.²⁹

In both instances, the military was called upon at points to aid what was at times an overwhelmed law enforcement community. See Figure 6.21.³⁰

Other questions regarding the dominance of federal authority as a natural hindrance to state involvement as to the National Guard have also been raised by the Rand Commission.³¹ Rand severely critiqued the command and control functionality during these crises and suggested alternative structures where the state authority takes the lead in the emergency response—even as to military resources. An example of this novel approach is evident in the suggested dual command structure for response shown in Figure 6.22.³²

Exactly how the military assists in the homeland arena is both complicated and innovative when compared with past practices. Aside from the defense of the soil from foreign armies and attackers, the military is being asked to be partners in the fight against terrorism—tackling nontraditional enemies. Common examples of civil cooperation are

Homeland Security



Figure 6.21 Ferguson, Missouri in 2014—Day 6. Police stand in the foreground watching protesters amid tear gas. (From Wikipedia. Used Per Creative Common 4.0. Uploaded August 17, 2014, by user Loavesofbread. No modifications made.)

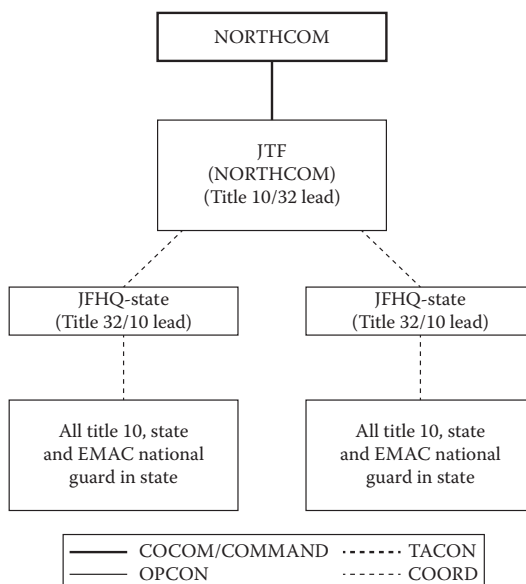


Figure 6.22 Dual-Status Command.

- Immediate response (any form of immediate action taken to save lives, prevent human suffering, or mitigate property damage under imminently serious conditions)
- Military support to civilian law enforcement agencies (loans of equipment, facilities, or personnel to law enforcement)
- Military assistance for civil disturbances
- Support for domestic counterterrorism operations
- Sensitive support operations

6.3 Fine Line of National Defense and Homeland Security

- Counterdrug operational support
- Terrorism consequence management (to include chemical, biological, radiological, nuclear, and high-yield explosive consequence management)
- Military support to civil authorities
- Support for civil disasters—natural or man-made (other than terrorism)
- Military cooperation with civil agencies
- Response under other authorities
- Oil or hazardous material spills
- Radiological emergencies/incidents
- Emergency water requirements
- Response to flooding
- Forest fire emergencies
- Mass immigration
- Transportation support³³

While this section cannot possibly cover every aspect of military cooperation, it will seek to address the most notable.

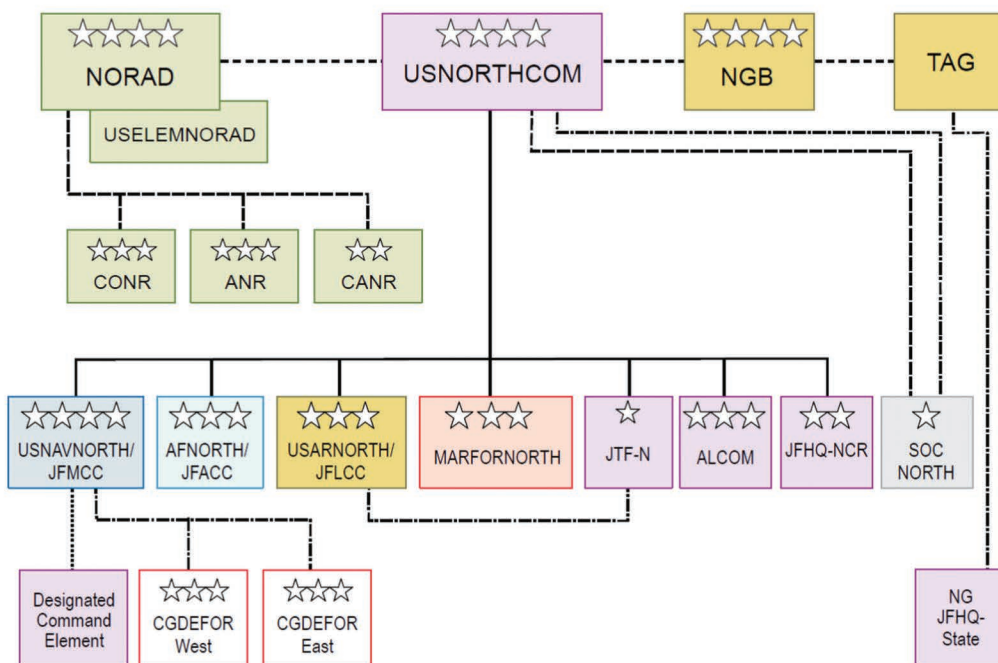
6.3.1 Department of Defense and Homeland Security

The defense of a nation fundamentally relies on its military infrastructure. Yet, in the affairs of homeland security, especially in a free society, the military sector cannot tackle the internal affairs of law enforcement and safety. That is not the military's integral mission. Nor is it the province of the military to meddle in the duties of state, local, or federal law enforcement—these being distinct and, for the most part, civilian counterparts and colleagues of the military. It is a delicate balance, with the DoD assuming primary control of the military confrontation that arises from foreign enemies and DHS and its aligned agencies and departments handling the internal affairs. The joint chiefs of staff for the military lay out the respective obligations. Put another way, it is simply impossible to separate the task of homeland defense from a military complex rich and mighty in its resources and capabilities. Everything, in the end, finds a nexus, a connection to the defense of the homeland. Figure 6.23³⁴ portrays how literally every component of the Northern Command of the U.S. military connects to this fundamental responsibility to protect our nation from every enemy including the terrorist. And within this same graphic, it is just as clearly evident that each branch of the service connects to each other branch to carry out the mission of homeland defense.

DoD is the lead, supported by other agencies, in defending against traditional external threats/aggression (e.g., air and missile attack). However, against internal asymmetric, nontraditional threats (e.g., terrorism), the DoD may be in support of DHS. When ordered to conduct HD operations within U.S. territory, the DoD will coordinate closely with other federal agencies or departments. Consistent with laws and policy, the services will provide capabilities to support combatant command requirements against a variety of air, land, maritime, space, and cyber incursions that can threaten national security. These include invasion, computer network attack, and air and missile attacks.

The purpose of HD is to protect against and mitigate the impact of incursions or attacks on sovereign territory, the domestic population, and defense critical infrastructure.³⁵

United States Northern Command Homeland Defense Command Relationships



Legend

AFNORTH	Air Force North	—————	combatant command (command authority)
ALCOM	United States Alaskan Command		supporting
ANR	Alaskan North American Aerospace Defense Command Region	—————	operational control
CANR	Canadian North American Aerospace Defense Command Region	-----	coordination
CGDEFOR	Coast Guard defense force	-----	direct support
CONR	continental United States North American Aerospace Defense Command Region		
JFACC	joint force air component commander		
JFHQ-NCR	Joint Force Headquarters-National Capital Region		
JFLCC	joint force land component commander		
JFMCC	joint force maritime component commander		
JTF-N	Joint Task Force-North		
MARFORNORTH	United States Marine Corps Forces, North		
NGB	National Guard Bureau		
NG JFHQ-State	National Guard joint force headquarters-state		
NORAD	North American Aerospace Defense Command		
SOCNORTH	United States Special Operations Defense Command, North		
TAG	the adjutant general		
USARNORTH	United States Army, North		
USELEMNORAD	United States Element, North American Aerospace Defense Command		
USNAVNORTH	United States Naval Forces, Northern Command		
USNORTHCOM	United States Northern Command		

Figure 6.23 U.S. Northern Command Homeland Defense Command Relationships.

A graphic portrayal of this series of interrelationships is shown in Figure 6.24.³⁶

These are distinct though very complementary missions. Since 9/11, those entrusted with military affairs have had to reconsider these traditional lines. Organizations like the DoD are by nature bureaucratically entrenched and slow to change. Moving away from the historic mission

6.3 Fine Line of National Defense and Homeland Security

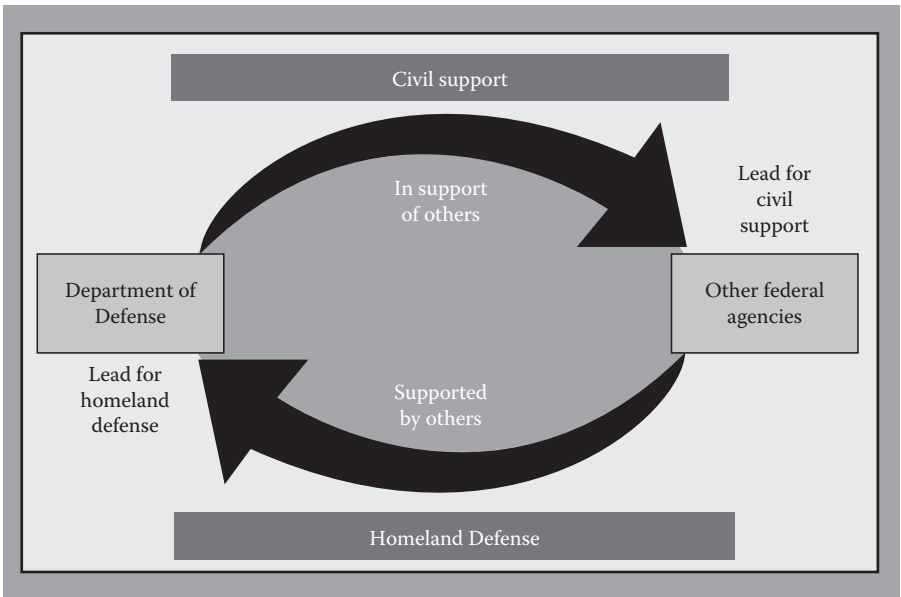


Figure 6.24 Lead federal agency and DoD relationships.

Strategic objectives
Reduce America’s vulnerability to terrorism Prevent terrorist attacks within the United States Minimize damage and recover from attacks that occur
Critical areas
Indications and warning Border and transportation security Domestic counterterrorism National critical infrastructure and key assets protection International cooperation Interoperability Emergency preparation and response

Figure 6.25 National strategy for homeland security strategic objectives and critical areas of concern.

will not occur readily, although in administrative agency time, the DoD has sprinted to this new vision—the view that the military plays a central role in the fight against terrorism. It is now safe to say that the DoD has blended the homeland function into the military model. In a recent study by the joint chiefs of staff, the merger is blatantly apparent³⁷ (see Figure 6.25).

In Iraq and Afghanistan, the military has assumed a major role in the provision of safety and security for these populations. It is not just the military tactic at play here but something dramatically larger—that of the safety and security of nation-states. At no place is this more obvious than in the reporting of deaths in Iraq, where the task of minimizing human harm and tragedy weighs heavily on military commanders and boots on the ground. At some stages of the Iraq campaign, the casualty rates were absolutely distressing, and public outcry raged over these

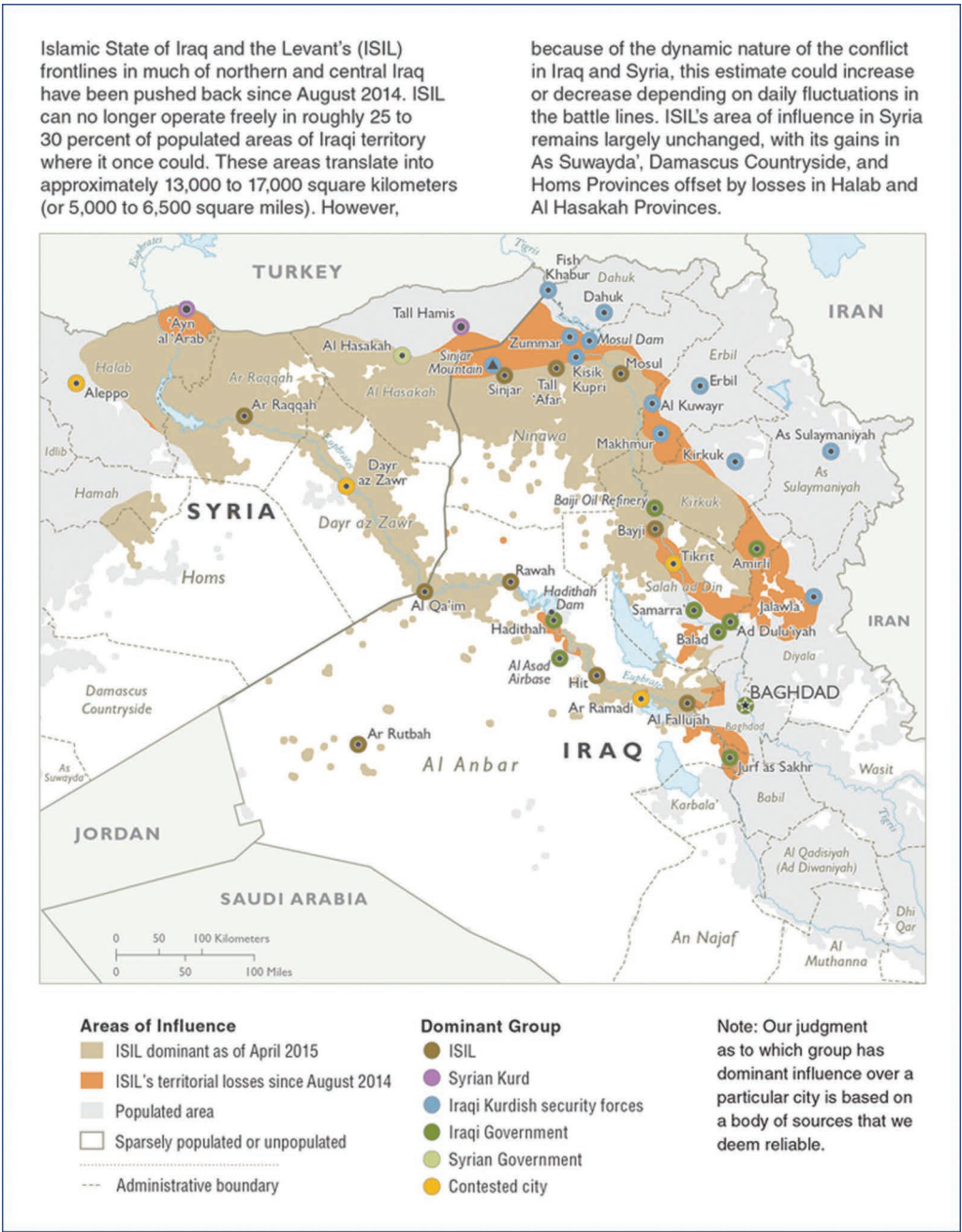


Figure 6.26 ISIL's reduced operating areas as of April 2015.

losses. Before the U.S. military left Iraq in 2012–2013, leaving only a small noncombatant force, the situation had dramatically improved, and with military adjustments, in both size and strategy, the unceasing and unmitigated levels of violence seemed to have halted.³⁸ However, in the vacuum left behind by U.S. military absence, the void was filled by forces known as the Islamic State of Iraq and Syria (ISIS). In Syria alone, nearly 200,000 people have perished in a horrible

6.3 Fine Line of National Defense and Homeland Security

civil war with poor prospects for near-term peace.³⁹ Whatever peace and tranquility existed in Iraq was surely replaced by the brutality and viciousness of ISIS (see Figure 6.26⁴⁰).

Despite the seeming impossibility of eradicating ISIS, U.S. policy decisions and the incisive use of the military have made an extraordinary, even striking difference in the power of ISIS. During Trump's tenure, ISIS's area of occupation and operation had been dramatically reduced. Compare Figure 6.27⁴¹ results and the most telling relates to a loss of controlled area. At last reports, plan to Islamicize the entire world has evaporated.

Internet Exercise: To update the figures on civilian deaths, visit <https://www.iraqbodycount.org/analysis/numbers/2014/>

In general, the DoD now thinks in terms of terror and a new war on nontraditional combatants. The DoD reported its numerous activities in the fight against terrorism in its Defend America program. Defend America has since been merged into the DoD general operations. However, DoD policy and pronouncement never strays far from the analysis of terror as it covers the Iraq, Syria, and Afghanistan campaigns. As the United States continues its slow but steady withdrawal from this region, the challenges of terror simply ebb and escalate. Even President Obama, who was severely resistant to any military involvement in the region, recognized that these threats know no boundaries. The Trump administration took steps to reduce troop presence in both Syria and Afghanistan. In the latter case, the war is the longest in the history of this nation and appears unwinnable in traditional military terms. And our enemies always adapt and adjust with new methods and means not previously encountered. With the Paris attacks in the fall of 2015 and San Bernardino attack in December 2015, it can be seen that ISIS seeks to aggressively recruit followers online and respects no nation or any geographic boundary. And the military campaign may be less likely than the use of vans, cars, trucks, machetes, and razors to achieve terror has become far too common.⁴²

At the same time, our military special ops continue their activities to ferret out the terrorist and to make sure these operators never make it to U.S. soil. The death of Abu Baghdadi was one of those remarkable raids that only our special forces could accomplish. See Figure 6.28.⁴³

Internet Exercise: Read about the life and time of Abu Baghdadi at <https://www.theguardian.com/world/2019/oct/27/abu-bakr-al-baghdadi-obituary>

A recently announced defense response, Operation Inherent Resolve, lists ISIS targets destroyed by means of airstrikes alone (see Figure 6.29⁴⁴).

The integration of the DoD into the affairs of terror and global threat can be gleaned from its own organizational changes. The DoD has erected a wide array of offices dedicated to this new war, designated and delineated its responsibility in specific instances of attack, and erected a new bureaucratic structure under the auspices of an assistant secretary of defense for homeland defense and global security—all of which targets terror and threat⁴⁵ (see Figure 6.30).

6.3.2 Intelligence Gathering and Sharing

All sectors of the military are now gathering, as well as sharing, intelligence information. Each of the four major branches has an intelligence arm that focuses its attention on threat and attack. Since 9/11, each sector has redirected part of its approach to the prevention of terrorism. A short sketch of each follows.

6.3.2.1 Office of Naval Intelligence

The Office of Naval Intelligence (ONI) deals with both historic and new challenges. Today, ONI's mission includes providing intelligence on the capabilities of foreign naval powers, providing global maritime intelligence integration supporting the global fight against terrorism, and enabling maritime domain awareness for HD. ONI's Civil Maritime Intelligence Division supports the disruption of maritime smuggling operations and the enforcement of international trade sanctions to deny terrorists use of the sea as a means of attack. Naval Intelligence—with

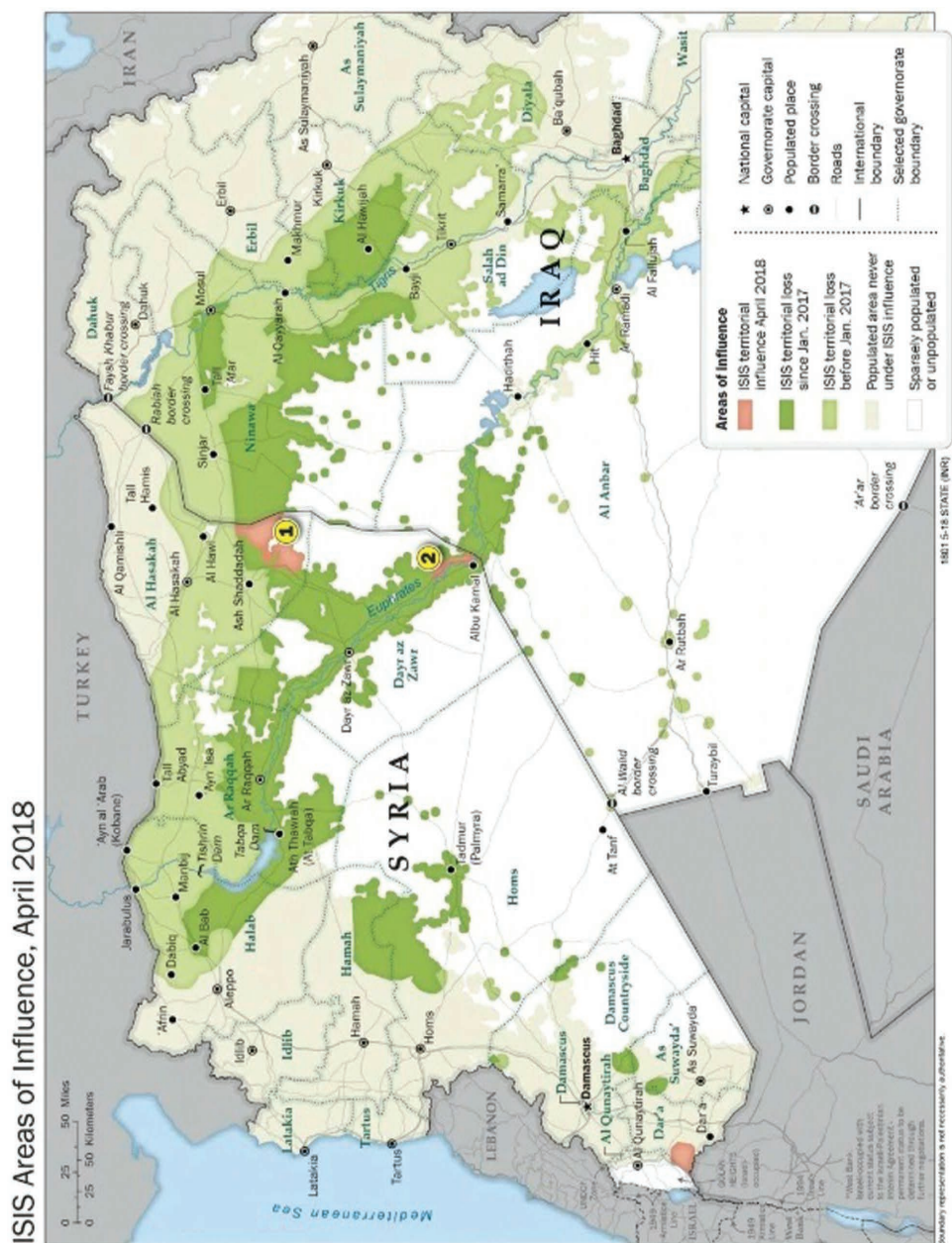


Figure 6.27 2018 map of ISIS's shrinking territory. (Source: U.S. Department of State.)

UNCLASSIFIED



(U) THE POSITIVE IDENTIFICATION OF ABU BAKR AL-BAGHDADI

- (U) **27 October 2019:** A Defense Intelligence Agency DNA laboratory processed DNA samples from the enemy killed-in-action suspected to be Abu Bakr al Baghdadi. The DNA analysis resulted in a direct match to a 2004 DNA sample collected at an Iraq detention center from Abu Bakr al-Baghdadi.
 - Statistical analysis indicates a probability of **1 in 104 Septillion** (1.04×10^{26}) to support this match.
- (U) For perspective, if the population of earth was 14.8 quadrillion times what it is today (~7 billion), you would still only expect to find one person with this DNA profile.



UNCLASSIFIED

Figure 6.28 The DIA positive identification confirming the death of Abu Baghdadi.



Figure 6.29 Targets damaged/destroyed as of December 9, 2015.

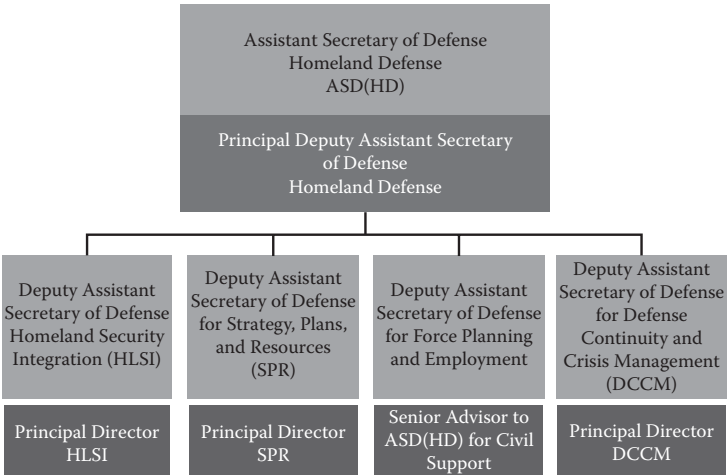


Figure 6.30 Organization chart of the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security.



Figure 6.31 NORAD Command Center. (Courtesy of U.S Air Force at Peterson.)



Figure 6.32 NORAD 60th anniversary logo.

Marine Corps Intelligence, the USCG, the Drug Enforcement Agency, and U.S. Customs—has also devoted an increased effort to nontraditional maritime intelligence missions.

6.3.2.2 Air Force Intelligence

While there has been some heated debate over the role of the air force in matters of HD, it appears that this branch of the service is crucial to success. Terrorism is now part of the air force mission. Dealing with this threat rests on many fronts, though none more essential than the work of the North American Aerospace Defense Command (NORAD), a binational U.S. and Canadian organization charged with providing aerospace warning and control for North America (Figure 6.31).

2020 marks the 60th anniversary of the NORAD defense program and the future cooperation between the United States and Canada looks equally bright. See Figure 6.32.

To accomplish this mission, NORAD uses a network of ground-based radars and fighters to detect, intercept, and, if necessary, engage any probable threat to the continent (see Figure 6.33).

The air force also operates a newly restructured intelligence center—the Air Force Intelligence, Surveillance, and Reconnaissance Agency. The Air Force Intelligence, Surveillance, and Reconnaissance Agency's headquarters is at Lackland Air Force Base, Texas, although the agency's 12,000 people serve at approximately 72 locations around the world. The agency's mission is to organize, train, equip, and present assigned forces and capabilities to conduct intelligence, surveillance, and reconnaissance for combatant commanders and the country. One tool of intelligence gathering has been the Predator drone, used by the navy in great quantity. Recently, the air force has been prompted to increase its production and capability in this area (Figure 6.34).

6.3 Fine Line of National Defense and Homeland Security



Figure 6.33 NORAD mission. (Courtesy of NORAD: Photo by: Staff Sgt. Perry Aston at <https://www.norad.mil/Images/igphoto/2002297858/>.)



Figure 6.34 The Air Force MQ-1B Predator.

Drones, while excellent intelligence tools, had caused a good deal of consternation among critics. Al-Qaeda, Taliban, and ISIS leaders have all been on the receiving end of the drone strike, but so have U.S. citizens working with the same groups who met early ends. Critics argue that the drone replaces due process for those Americans who are simply executed in the theatre of war.⁴⁶

6.3.2.3 U.S. Marine Corps

While the U.S. Marine Corps (USMC) is under the operational control of the navy, it has constructed a plethora of intelligence organizations and operational programs relevant to the fight against terrorism. The Corps also has a bevy of Intelligence Schools and training facilities throughout its bases and aligned operations at the Pentagon.

Internet Exercise: Find out about the Marine Corps Intelligence Schools and Career tracks for officers at <https://www.trngcmd.marines.mil/Northeast/MCIS/About-Us/>

Homeland Security

At its marine base in Quantico resides its intelligence headquarters, with its primary functions being to

- Discharge Marine Corps responsibilities for intelligence estimates, plans, reports, and studies
- Review, analyze, and coordinate joint papers that pertain to Marine Corps intelligence matters
- Recommend positions for approval and use by the Commandant of the Marine Corps (CMC) and the Headquarters of the Marine Corps (HQMC) staff
- Develop plans, policies, operational concepts, doctrine, and techniques in the fields of intelligence, counterintelligence, and cryptologic/signals intelligence in coordination with staff agencies
- Coordinate with the HQMC staff to develop plans and policies

The Marine Corps developed a cultural studies program for its professional and enlisted class as it seeks to understand and converse with both friendly citizens and the combatant enemy. The commandant of the Marine Corps, in his Vision and Strategy for 2025, states that the corps “will go to great lengths to understand enemies and the range of cultural, societal and political factors affecting all people Marines interact with.”⁴⁷

The USMC Center for Advanced Operational Culture Learning (CAOCL) promotes a grasp of culture and language as regular, mainstream components of the operating environment—the human terrain—throughout the full spectrum of military operations and is the Corps’s one-stop clearinghouse for operational culture and language training. CAOCL is now fully integrated into the Marine Corps University⁴⁸ (see Figure 6.35).

The Marine Corps Regional, Cultural, and Language Familiarization (RCLF) program ensures that marines are equipped with operationally relevant regional, cultural, and language knowledge to allow them to plan and operate successfully in the joint and combined expeditionary environment

- In any region of the world
- In current and potential operating conditions
- Targeting persistent and emerging threats and opportunities

The Marine Corps employs distance education techniques in its portal, Marine.net. A recent sampling of courses pertinent to homeland security include

- Cultural Awareness and Terrorism
- Risk Management: Organization Risk and Safety and Health Legislation



Figure 6.35 USMC Center for Advanced Operational Culture Learning (CAOCL).

- Joint Anti-Terrorism Level 1
- Threat Levels and Force Protection Conditions
- Terrorism Awareness
- Stability and Support Operations
- Physical Security Specialist
- Physical Security Chief
- National and International Security Studies

6.3.2.4 U.S. Army

The U.S. Army established its own security command—the U.S. Army Intelligence and Security Command (INSCOM). INSCOM conducts intelligence, security, and information operations for military commanders and national decision makers. Headquartered at Fort Belvoir, Virginia, INSCOM is a global command with ten major subordinate commands and a variety of smaller units with personnel dispersed over 180 locations worldwide (see Figure 6.36).

The subordinate commands are:

1st Information Operations Command (Land)

The first IO Command is the only Army full-spectrum IO organization engaged from information operations theory development and training to operational application across the range of military operations.

66th Military Intelligence Brigade

The 66th MI Brigade conducts theater-level multidiscipline intelligence and security operations and, when directed, deploys prepared forces to conduct joint/combined expeditionary and contingency operations in support of U.S. Army Europe and U.S. European Command.

116th Military Intelligence Brigade

The 116th MI Brigade conducts 24/7 tasking, collection, processing, exploitation, dissemination, and feedback operations of multiple organic and Joint aerial-intelligence surveillance and reconnaissance (A-ISR) missions collected in overseas contingency areas of operation.

207th Military Intelligence Brigade

The 207th Military Intelligence Brigade (MIB) Theater (T) conducts intelligence analysis, collection, and exploitation in support of U.S. Army Africa (USARAF) and U.S. Africa Command (USAFRICOM) in order to set the intelligence architecture for the theater, disrupt transnational and transregional threats, and promote regional stability in Africa while building and maintaining intelligence readiness.



Figure 6.36 INSCOM logo.

Homeland Security

470th Military Intelligence Brigade

The 470th MI Brigade provides timely and fused multidiscipline intelligence in support of U.S. Army South, U.S. Southern Command, and other national intelligence agencies.

500th Military Intelligence Brigade

The 500th Military Intelligence Brigade (Theater) conducts multidiscipline intelligence collection and analysis and sets the theater for intelligence for U.S. Army Pacific (USARPAC) within the U.S. Indo-Pacific Command area of responsibility, in order to provide timely, predictive intelligence to enable commander decision-making.

501st Military Intelligence Brigade

The 501st MI Brigade conducts theater-level multidiscipline intelligence for Joint and Combined Warfighters from the Republic of Korea.

513th Military Intelligence Brigade

The 513th Military Intelligence Brigade (Theater) provides tailored, multidisciplined intelligence and intelligence capabilities in support of USARCENT and other commands' execution of Unified Land Operations in the USCENTCOM AOR.

704th Military Intelligence Brigade

The 704th Military Intelligence Brigade provides trained and ready forces to conduct global cryptologic operations for the National Security Agency and Army and Joint commanders.

706th Military Intelligence Group

The 706th Military Intelligence Group provides trained and ready Soldiers and Civilians in order to enable National Security Agency (NSA)/Central Security Service (CSS) Georgia cryptologic operations supporting regional intelligence activities and globally deployed U.S. Forces with accurate and timely Signals Intelligence (SIGINT).

780th Military Intelligence Brigade

The 780th conducts cyberspace operations to deliver effects in support of Army and Joint requirements.

902nd Military Intelligence Group

The 902nd Military Intelligence Group provides direct and general counterintelligence support to Army activities and major commands. The group also provides general support to other military department counterintelligence and intelligence elements, unified commands, defense agencies, and national agency counterintelligence and security activities and organizations.

Army Field Support Center (AFSC)

AFSC provides specialized operational, administrative, and personnel management support to Department of the Army and other Department of Defense Services and Agencies as directed.

Army Operations Group (AOG)

USAOG conducts and enables global contingency full-spectrum Human Intelligence (HUMINT) operations in support of U.S. Army intelligence and operational requirements. USAOG enhances and sustains U.S. Army HUMINT skill sets as the U.S. Army functional HUMINT Foundry lead.

National Ground Intelligence Center (NGIC)

NGIC is the Defense Department's primary producer of ground forces intelligence.

Internet Exercise: Visit the INSCOM web location for a full view of the Army Intelligence Service. <https://www.inscom.army.mil/msc/>

6.3.2.5 United States Coast Guard Intelligence

The unique mission and overall tasks of the United States Coast Guard make the organization's intelligence gathering crucial to homeland defense. By its essential nature, the Coast Guard protects the natural borders of the entire nation as well as its ports, harbors, bays, rivers, and points of entry where terror always remains a possibility. As a result of this crucial role in homeland defense, the Coast Guard, as other governmental entities and military branches, now shares and collaborates across the intelligence community. The mission of the United States Coast Guard Intelligence is multifaceted:

- Conduct intelligence activities to provide timely, objective, relevant, and actionable maritime intelligence
- Use intelligence in the development of policy and protocol
- Employ intelligence to drive operations and enable mission support
- Utilize intelligence to make informed decision-making for Coast Guard and Homeland Security missions and National Security requirements.⁴⁹

See Figure 6.37.

The Coast Guard Intelligence office divides into three divisions, namely:

- Counterintelligence Service
- Coast Guard Cryptologic Group
- Intelligence Coordination Center

Of extraordinary interest is the Coast Guard Cryptologic analysis which includes the analysis and interpretation of signals intelligence to prevent, deter, and threat terrorist or criminal activity in its usual spheres of operations including rivers, waterways, and especially the high coast sea lines. The unit picks up the transmissions as it scans the messaging. See Figure 6.38.



Figure 6.37 U.S. Coast Guard Intelligence logo.



Figure 6.38 The U.S. Coast Guard Cryptologic Group logo.



Figure 6.39 National Maritime Intelligence-Integration Office.

Internet Exercise: Visit the U. S. Coast Guard's Intelligence service at <https://www.dco.uscg.mil/Our-Organization/Intelligence-CG-2/>

6.3.3 Specialized Military/Defense Units Dedicated to Homeland Security

There are simply too many military entities and groups to enumerate that relate to the world of homeland security. Each branch of the service dedicates some portion of its resources to the fight against terrorism, and each lends its expertise to particular tasks and challenges. This section will cover representative examples of these military contributions.

6.3.3.1 National Maritime Intelligence-Integration Office (NMIO)

Primarily a center for naval intelligence, the NMIO's resources and information are available to all branches of the military and the USCG. The NMIO is home to the ONI and is the central location for maritime intelligence (Figure 6.39).

NMIO displays a narrow intelligence interest though it has a global vision and approach. Threats are assessed and evaluated in the maritime environment rather than the whole framework in which threats occur. Hence, NMIO targets threats in these basic categories:

Asymmetric: Terrorism, WMD proliferation, cyber attack, global supply chain disruption, and so on

Criminal/illicit activities: Maritime piracy, narcotics and contraband smuggling, human trafficking, illegal exploitation of marine resources, and so on

Environmental destruction: Toxic waste, illegal dumping, overfishing, and so on⁵⁰

See Figure 6.40.

Located in Suitland, Maryland, NMIO supports joint operational commanders with a worldwide organization and an integrated workforce of active duty, reserve, and civilian personnel. NMIO supports the navy's acquisition activities by providing scientific and technical analysis of naval weapons systems.

NMIO also offers a variety of training courses that are fully online, and which lay out the unique challenges of the maritime industry when dealing with security.

Internet Exercise: To review an NMIO training class on the Maritime Industry, see: <https://nmio.port.training/>

6.3.3.2 National Reconnaissance Office

Coordinating reconnaissance activities is the DoD's National Reconnaissance Office (NRO). The NRO designs, builds, and operates the country's reconnaissance satellites. NRO products, provided to an expanding list of customers such as the Central Intelligence Agency (CIA) and the DoD, can warn of potential trouble spots around the world, help plan military operations,

6.3 Fine Line of National Defense and Homeland Security

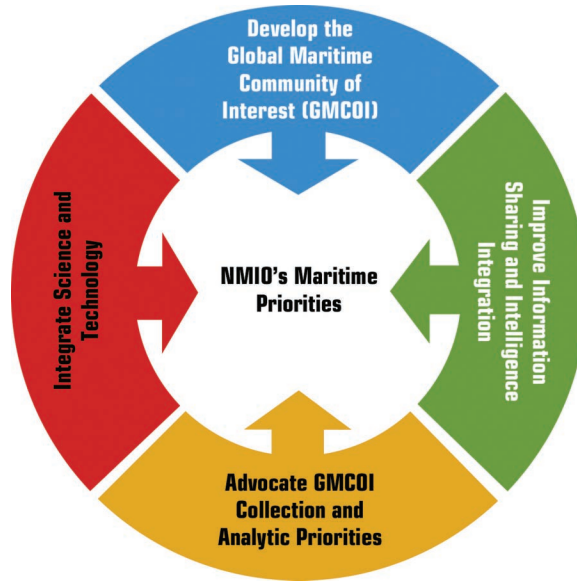


Figure 6.40 Diagram illustrating the components that comprise the NMIO's Maritime priorities.



Figure 6.41 National Reconnaissance program, part of the National Foreign Intelligence program.

and monitor the environment. A DoD agency, the NRO is staffed by DoD and CIA personnel. It is funded through the National Reconnaissance program, part of the National Foreign Intelligence program (see Figure 6.41).

Internet Exercise: Find out about the many career option in NRO at <https://www.nro.gov/Careers-and-Internships/Career-Fields/>

6.3.3.3 Weapons of Mass Destruction Civil Support Teams

The U.S. Army and the National Guard play a central role in the WMD protocol. Civil Support Teams (CSTs) aid civilian authorities with military expertise regarding chemical, biological, radiological, and nuclear materials (Figure 6.42).

The CST was designed to augment local and regional terrorism response capabilities in events known or suspected to involve the use of chemical, biological, or radiological agents. The team can be en-route within 3 hours to support civil authorities in the event or suspicion of a WMD attack. Specifically, the CST deploys to an area of operations to

- Support civil authorities to identify chemical, biological, radiological, and nuclear agents/substances



Figure 6.42 Civil Support Team.



Figure 6.43 Soldiers and Airmen of the Maryland National Guard's 32nd Weapons of Mass Destruction-Civil Support Team train aboard the USS Barry March 6 at the Washington Naval Yard during Exercise Capital Spear. (Photo by Tech. Sgt. Mike R. Smith, National Guard Bureau.)

- Assess current and projected consequences
- Advise on response measures
- Assist with mitigation and additional support

The role of the U.S. military in the matter of WMD has been essential. The sharing and collaboration between civil authorities seem almost natural and without equivocation. Given the seriousness of the subject matter, both the army and public authorities share a similar vision regarding WMD. See Figure 6.43.

The DoD, working in unison with non-military authorities, seeks to minimize WMD at every level, from pure prevention to total eradication. In Figure 6.44,⁵¹ the goals of its overall efforts are charted as *End States*.

The U.S. Army lays out its operational approach, which is clearly collaborative⁵² (see Figure 6.45).

6.3 Fine Line of National Defense and Homeland Security

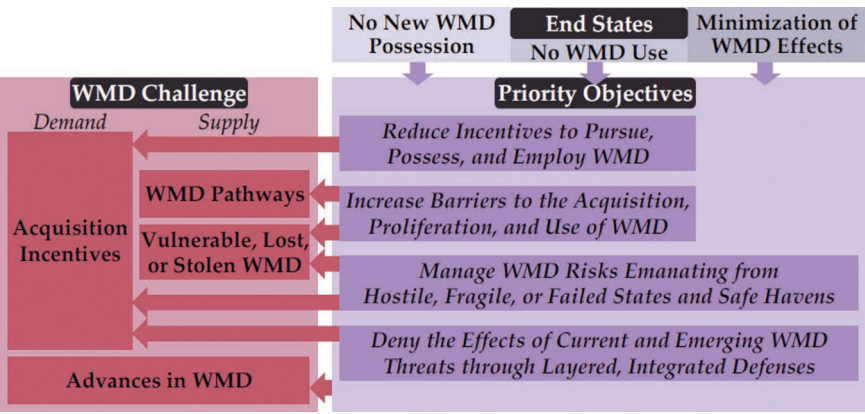


Figure 6.44 End states, priority objectives, and the WMD challenge.

1. U.S. Armed Forces, in concert with other elements of U.S. national power, deter WMD use.
2. U.S. Armed Forces are prepared to defeat an adversary threatening to use WMD and prepare to deter follow-on use.
3. Existing worldwide WMD is secure and the U.S. Armed Forces contribute as appropriate to secure, reduce, reverse or eliminate it.
4. Current or potential adversaries are dissuaded from producing WMD.
5. Current or potential adversaries' WMD is detected and characterized and elimination sought.
6. Proliferation of WMD and related materials to current and/or potential adversaries is dissuaded, prevented, defeated or reversed.
7. If WMD is used against the United States or its interests, U.S. Armed Forces are capable of minimizing the effects in order to continue operations in a WMD environment and assist United States civil authorities, allies and partners.
8. U.S. Armed Forces assist in attributing the source of attack, respond decisively, and/or deter future attacks.
9. Allies and U.S. civilian agencies are capable partners in combating WMD.

Figure 6.45 U.S. Armed Forces WMD strategy.

Initially located in the U.S. Strategic Command, the center has been aligned with the Defense Threat Reduction Agency (DTRA). The center provides recommendations to dissuade, deter, and prevent the acquisition, development, or use of WMD and associated technology. Through collaboration with the United States and allied organizations, the center provides situational awareness of worldwide WMD and related activities, as well as providing day-to-day and operational crisis support via the operations center. DTRA has played an active and ongoing role in the COVID-19 response. Figure 6.46⁵³ portrays a very active involvement in seeking to minimize the threat of this pandemic.

Among its responsibilities are

- *Partnering*: Using our unique expertise, we are developing and strengthening the CWMD capabilities of our allies, partner nations, the military, and other federal, state, and local government agencies.



Figure 6.46 The DTRA's global partners and training initiatives.



Figure 6.47 DTRA symbol at headquarters entrance.

- *Verifying*: Treaties, conventions, documents on WMD—our WMD experts travel the globe to inspect, assess, and verify that these international agreements on WMD are being upheld.
- *Researching*: WMD threats are constantly changing, evolving—and new threats emerge unexpectedly. Our dedicated R&D efforts are combating today’s WMD—and developing solutions to future threats.
- *Responding*: Whether dealing with intentional WMD use, or a natural or accidental chemical, biological, radiological, and nuclear (CBRN) incident, someone needs to be prepared to deal with a worst-case scenario—and that someone is us.
- *Defending*: Our adversaries fall into two categories: those who have WMD, and those who want them. We must be able to defend the warfighter, our country, and our allies from WMD—here and abroad.
- *Preparing*: There is no second chance to stop WMD—which is why we are constantly training, testing, and planning. We take this approach with ourselves, our military, and our international partners.
- *Nuclear support*: Safe. Secure. Effective. The United States’ nuclear arsenal needs to be all three—and we are responsible for ensuring that these three conditions are met, every day, around the world.

The Defense Threat Reduction Agency (DTRA) is a combat support agency of the U.S. DoD (Figure 6.47).

Founded in 1998, the agency headquarters is located in Fort Belvoir, Virginia. DTRA employs over 2,000 men and women, both military and civilian, at more than 14 locations around the world.

Internet Exercise: Discover where DTRA is located globally. Do you see logic in these locations? Visit <https://www.dtra.mil/About/DTRA-Locations/>.

The DTRA safeguards America and its allies from WMDs (CBRN and high explosives) by providing capabilities to reduce, eliminate, and counter the threat and to mitigate its effects. It is sometimes designated as the strategic command of WMD.

Homeland Security

The DTRA expends a considerable portion of its time and energy on conducting basic scientific research regarding WMD. It uses “science to secure WMD.” All of DTRA’s research encompasses five basic lines of inquiry:

- Basic and applied science
- Chemical/biological technologies
- Counter-WMD technologies
- Nuclear technologies
- Information sciences and applications

DTRA’s research seeks

- To improve scientific knowledge that supports verification of treaties, safeguards, and nonproliferation
- To safely handle, transport, secure, or eliminate WMD components and weapons; and use novel means that lead to physical or other methods to monitor compliance and reduce illegal proliferation pathways
- To advance capabilities for safe and verifiable control of materials, systems, and facilities that underpin greater confidence for entering, exiting, or sustaining multinational WMD-related agreements⁵⁴

6.4 Conclusion

The chapter scrutinizes how homeland functions need governmental collaboration.⁵⁵ DHS alone cannot carry out the multitude of homeland functions. The chapter urges practitioners to see wisdom in the mutual support of local, state, and federal agencies in the fight against terrorism. On top of this, from its earliest days of inception, DHS fostered an environment of decentralization over centralization—concluding that local officials understood the demands and dynamics of their constituencies better than removed bureaucrats. The political and structural intermix and interdependency of homeland security is the chief emphasis of this chapter. Not exclusively a federal obligation, the content lays out the mandatory and absolute need for state and local cooperation. The various state departments are highlighted, with some of the better examples of state homeland offices being fully covered. How states and localities structure the homeland mission and carry out the aligned tasks of homeland is a crucial topic. Special emphasis on the use of task forces and coordinating committees is provided in the chapter, as well as discussion of the novel innovation known as the fusion center. In addition, the reader will encounter the growing local role in homeland security. In a continuous move to decentralization, the locality, whether county or city, is increasingly called upon to deliver services to the homeland quarter. Fusion centers are covered too, where intelligence is disseminated at regional levels throughout the United States. Presently, there are 58 fusion centers in the United States. Other programs that foster the collaboration of governmental entities include Citizen Corps, Community Emergency Response Teams (CERTs), the Fire Corps, and Volunteers in Public Service.

The chapter distinguishes the differing yet complementary roles of our national security mission, the military intelligence complex, and DHS. How the branches of our military complex serve the country is narrowly covered in light of the terrorist threat. Since military commands throughout the world deal with a host of homeland issues, the line between the two forces tends to merge rather than remain separate. The military itself divides up its responsibility to now include combatant zones with HD considerations. Homeland personnel rely on air force equipment and mission activity to secure the borders. FEMA regularly depends on military capacity

to serve those victimized by natural disaster. The entire DoD has integrated homeland functions into its mission and purpose. Some even argue that the present campaigns in Iraq and Afghanistan are merely extensions of the HD strategy. Surely the missions are complementary, though not identical. Both DHS and the military are concerned with intelligence and information gathering. The chapter highlights the more prominent programs of the major military branches dedicated to homeland questions. The line between military defense and homeland defense easily merges or crosses over. Coverage also includes a quick look at emergent departments and entities dedicated to the mix of the military and the homeland, such as the National Maritime Intelligence Center, the NRO, and the Center for Combating Weapons of Mass Destruction.

Keywords

Adjutant General; Center for Advanced Operational Culture Learning; Citizen Corps Council; Civil Support Teams; Combatant Zone; Cultural Studies Program; Decentralization; Defend America; Defense Threat Reduction Agency; Fusion Center; Ground-Based Radar; Infrastructure Protection Program; Intelligence and Security Command; Intelligence Officer; Intelligence Surveillance and Reconnaissance Agency; Joint Chiefs of Staff; Law Enforcement Terrorism Prevention Program; Metropolitan Area; Military Incursion; Military Tactic; National Foreign Intelligence Program; National Guard; National Infrastructure Protection Plan; National Maritime Intelligence Center; National Preparedness Guidelines; National Reconnaissance Office; North American Aerospace Defense Command; Office of Intelligence and Analysis; Office of Naval Intelligence; Predator Drone; Public Safety Interoperable Communications Grant Program; Public Works; Regional Planning Council; Sovereign Territory; State Homeland Security Director; State, Local, Tribal, and Territorial Government Coordinating Council; Task Force; U.S. Strategic Command; Unified Command; Urban Area Security Initiative Grant program; Working Group

Discussion Questions

1. What is the purpose and aim of the fusion center?
2. How do DHS funding and grants manifest the department's preference for local input and implementation?
3. Describe three DHS program initiatives that signify the importance of local control and involvement.
4. When does the line between military command and services become muddled with the services of DHS?
5. Discuss the diverse ways in which the military commands make contributions to the fight against terrorism.
6. Explain how the typical state might garner funding for homeland security and deliver its services.
7. Relay two major challenges to the idea of state, local, and federal cooperation in the world of homeland security.
8. Is it a fair conclusion to hold that DHS prefers decentralization over centralization of services?

Homeland Security

9. What is the best argument for local initiative in the delivery of homeland services?
10. Give three examples of DHS programs or policies that encourage intergovernmental cooperation.

Practical Exercises

1. Contact your regional or state Office of Homeland Security. List five initiatives of this office.
2. Discover whether Citizen Corps works in your community. If so, explain its current endeavors.
3. Interview a state DHS official. Try to discern how positive this office's relation to and with DHS is.
4. Discover at least two different funding sources for local implementation of homeland security activities.

Notes

- 1 Department of Homeland Security, Homeland Security Advisory Council, *Report from the Task Force on State and Local Homeland Security Funding* 15, June 2004.
- 2 National Governors Association, Homeland Security & Public Safety Committee, <http://www.nga.org/cms/center/hsp> (accessed August 13, 2020).
- 3 R. E. Brooks, *Improving Criminal Intelligence Sharing: How the Criminal Intelligence Coordinating Council Support Law Enforcement and Homeland Security* 34, February 2011.
- 4 Office of the President, *Homeland Security Presidential Directive 5*, February 2003, 6.
- 5 See CISA, State, Local, Tribal, and Territorial Government Coordinating Council Working Groups Webpage, <https://www.cisa.gov/slittgcc-working-groups> (accessed August 13, 2020).
- 6 See also: State of Louisiana, Governor's Office of Homeland Security & Emergency Preparedness, <https://gohsep.la.gov/PREVENT/OVERVIEW> (accessed August 13, 2020).
- 7 New York State, *Homeland Security Strategy 2014–2016*, https://dmna.ny.gov/training_and_exercises/j5/General%20Interest/NYS_Homeland_Security_Strategy_20140313.pdf (accessed August 13, 2020). See also: New York State, *Homeland Security Strategy 2017–2020*, <http://www.dhses.ny.gov/media/documents/NYS-Homeland-Security-Strategy.pdf> (accessed August 13, 2020).
- 8 New York State, *Homeland Security Strategy 2014–2016*, 48, https://dmna.ny.gov/training_and_exercises/j5/General%20Interest/NYS_Homeland_Security_Strategy_20140313.pdf (accessed August 13, 2020). See also: New York State, *Homeland Security Strategy 2017–2020*, <http://www.dhses.ny.gov/media/documents/NYS-Homeland-Security-Strategy.pdf> (accessed August 13, 2020).
- 9 New York State, *Homeland Security Strategy 2017–2020*, <http://www.dhses.ny.gov/media/documents/NYS-Homeland-Security-Strategy.pdf> (accessed August 13, 2020).
- 10 A. R. Agnes, Homeland Security/Emergency Management Budgets by Each U.S. State: Why do some states allocate so much more money than others do? *Political Science* 26 (2018): 33–36, https://scholar.archive.library.albany.edu/honorscollege_pos/26.
- 11 State of Tennessee, *Office of Homeland Security*, <https://www.tn.gov/safety/homeland-security.html> (accessed August 13, 2020).
- 12 See: State of Tennessee, Cyber Reference Aid, https://www.tn.gov/content/dam/tn/safety/documents/Cyber_Reference_Aid_09_OCT_13.pdf (accessed August 13, 2020).
- 13 Tennessee Fusion Center, Tactical Report, Cyber safety tips, https://www.tn.gov/content/dam/tn/safety/documents/Cyber_Safety_Tips_14_OCT_13.pdf (accessed August 13, 2020); See the excellent presentation on cyber security challenges and the protocols to minimize said threats at: Office of the Director of National Intelligence, A Common Cyber Threat Framework: A Foundation for Communication, <https://info.publicintelligence.net/ODNI-CyberThreatFramework.pdf> (accessed

- August 13, 2020); see also: National Governors Association Brief: Enhancing Role of Fusion Centers in Cybersecurity, July 19, 2015, <https://publicintelligence.net/nga-fusion-centers-cyber/> (accessed August 13, 2020).
- 14 D. E. Marks and I. Y. Sun, The impact of 9/11 on organizational development among state and local law enforcement agencies, *Journal of Contemporary Criminal Justice*, 23 2007: 159–173.
 - 15 B. R. Johnson, Fusion centers: Strengthening the nation's homeland security enterprise, *Police Chief*, February 2011: 62.
 - 16 US Department of Homeland Security, The National Network of Fusion Center: Where We Have Been and Where We are Going, page 6, <https://info.publicintelligence.net/DHS-FusionCenters.pdf> (accessed August 13, 2020).
 - 17 DHS, 2010 baseline capabilities assessment of fusion centers and critical operational capabilities gap mitigation strategy, <http://www.dhs.gov/2010-baseline-capabilities-assessment-fusion-centers> (accessed August 13, 2020).
 - 18 D. Keyer, Nationwide SAR initiative delivers value to fusion centers, *Police Chief*, February 2011: 40.
 - 19 National Strategy for the National Network of Fusion Centers 2014–2017 (March 29, 2015), <https://publicintelligence.net/national-fusion-center-strategy-2014-2017/> (accessed August 13, 2020).
 - 20 Ibid.
 - 21 US Department of Homeland Security, Office of Intelligence & Analysis, <https://www.dhs.gov/office-intelligence-and-analysis> (accessed August 13, 2020).
 - 22 See: US Department of Homeland Security, 2017 National Network of Fusion Centers: Final Report, <https://www.archives.gov/files/isoo/oversight-groups/sltps-pac/2017-national-network-of-fusion-centers-final-report.pdf> (accessed August 13, 2020).
 - 23 See Fusion Center Locations and Contact Information, <http://www.dhs.gov/fusion-center-locations-and-contact-information> (accessed August 13, 2020).
 - 24 Intelligence Fusion Centers, Fusion Centers Map, Locations, Contact Information (February 15, 2011), <https://publicintelligence.net/fusion-centers/> (accessed August 13, 2020).
 - 25 US Department of Homeland Security, Fusion Center Locations and Contact Information, <https://www.dhs.gov/fusion-center-locations-and-contact-information> (accessed August 13, 2020).
 - 26 See: Ready.gov, Citizen Corps, <https://www.ready.gov/citizen-corps> (accessed August 13, 2020).
 - 27 Library of Congress, The world with commanders' areas of responsibility map, <https://www.loc.gov/item/2005633566/> (accessed August 13, 2020).
 - 28 US Department of Defense, Combatant Commands, <https://www.defense.gov/Our-Story/Combatant-Commands/> (accessed August 13, 2020).
 - 29 Sgt. 1st Class Whitney Huges, More Than 4,000 Guard Members on Duty in DC, Christian Science Monitor, June 6, 2020, <https://www.nationalguard.mil/News/Article/2210590/more-than-4000-guard-members-on-duty-in-dc/> (accessed November 24, 2020).
 - 30 C. Guensburg, National Guard Deployments for Civil Unrest Uncommon in US, August 18, 2014, Voice of America, <https://www.voanews.com/usa/national-guard-deployments-civil-unrest-uncommon-us> (accessed August 13, 2020).
 - 31 L. E. Davis, J. Rough, G. Cecchine, A. G. Schaefer, and L.-L. Zeman, *Hurricane Katrina: Lessons for Army Planning and Operations*, RAND Corporation (2007), http://www.rand.org/content/dam/rand/pubs/monographs/2007/RAND_MG603.pdf (accessed August 13, 2020).
 - 32 Ibid. See also: Department of Defense: Joint Chiefs of Staff, Joint Publication 3–27, Homeland Defense, April 10, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_27.pdf (accessed August 13, 2020).
 - 33 S. J. Tomisek, Homeland security: New role for defense, *Strategic Forum (Institute for National Strategic Studies)*, 189, February 2002.
 - 34 Department of Defense: Joint Chiefs of Staff, Joint Publication 3–27, Homeland Defense, II–7, April 10, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_27.pdf (accessed August 13, 2020).
 - 35 Department of Defense: Joint Chiefs of Staff, *Joint Publication 3–26: Homeland Security*, August 2005, viii, http://www.fas.org/irp/doddir/dod/jp3_26.pdf (accessed August 13, 2020).
 - 36 Joint Chiefs, *Homeland Security*, II–17.
 - 37 Joint Chiefs, *Homeland Security*, I–2.
 - 38 Department of Defense, *Measuring Stability and Security in Iraq: Report to Congress in Accordance with the Department of Defense Appropriations Act 2008*, June 28, 2011.

Homeland Security

- 39 The Syrian Observatory for Human Rights now calculates the dead in the Syrian War to be in excess of 586,000. See: <https://www.syriahr.com/en/152189/> (accessed August 13, 2020).
- 40 U.S. DoD, Operation Inherent Resolve, http://www.defense.gov/News/Special-Reports/0814_Inherent-Resolve (accessed August 13, 2020).
- 41 See: Institute for the Study of War, ISIS Operating Areas, August 19, 2019, http://www.understandingwar.org/sites/default/files/ISIS%20Sanctuary%20Map%20AUG%202019_6.jpg (accessed August 13, 2020).
- 42 See: Laurence Norman, Belgium Launches Terror Probe as ISIS Claims Machete Attack Assailant was a 33-year-old Algerian man, federal prosecutors say (August 7, 2016), *The Wall Street Journal*, <https://www.wsj.com/articles/belgium-launches-terror-investigation-into-charleroi-machete-attack-1470570832> (accessed August 13, 2020).
- 43 U.S. Dept of Defense, Baghdadi Info Webpage, <https://media.defense.gov/2019/Oct/30/2002203987/-1/-1/0/191030-D-ZZ999-007.JPG> (accessed August 23, 2020).
- 44 U.S. DoD, Operation Inherent Resolve, http://www.defense.gov/News/Special-Reports/0814_Inherent-Resolve (accessed August 13, 2020).
- 45 Joint Chiefs, *Homeland Security*, II–6. See also: US Department of Defense, Assistant Secretary for Defense for Homeland Defense and Global Security Webpage, <https://policy.defense.gov/OUSSDP-Offices/ASD-for-Homeland-Defense-Global-Security/> (accessed August 13, 2020).
- 46 M. Sohn, Drone strikes and due process: The role of the separation of powers in Lethal action against U.S. citizens outside traditional battlefields, *Jolt Digest*, <https://jolt.law.harvard.edu/digest/drone-strikes-and-due-process> (March 6, 2013) (accessed August 13, 2020); see also W. Funk, Deadly drones, due process, and the fourth amendment, 22 *Wm & Mary Bill of Rights* (2013).
- 47 Cpl. G. Gonzalez, *CAOCL Helps Marines Navigate through 'Cultural Terrain'*, <https://www.pendleton.marines.mil/News/News-Article-Display/Article/536744/caocl-helps-marines-navigate-through-cultural-terrain/> (accessed August 13, 2020).
- 48 For more information on CAOCL, visit <https://www.usmcu.edu/CAOCL/>.
- 49 See: US Coast Guard, Intelligence, <https://www.dco.uscg.mil/Our-Organization/Intelligence-CG-2/> (accessed August 13, 2020).
- 50 National Maritime Intelligence-Integration Office, About NMIO, <https://nmio.ise.gov/About-NMIO/NMIO-Background/> (accessed August 13, 2020).
- 51 DOD, *Department of Defense Strategy for Countering Weapons of Mass Destruction* 7 (2014), http://archive.defense.gov/pubs/DoD_Strategy_for_Countering_Weapons_of_Mass_Destruction_dated_June_2014.pdf (accessed August 13, 2020).
- 52 Chairman of the Joint Chiefs of Staff, *National Military Strategy to Combat Weapons of Mass Destruction*, February 4, 2006; DoD, *Department of Defense Strategy for Countering Weapons of Mass Destruction* 7 (2014), http://archive.defense.gov/pubs/DoD_Strategy_for_Countering_Weapons_of_Mass_Destruction_dated_June_2014.pdf (accessed August 13, 2020).
- 53 Defense Threat Reduction Agency, COVID-19 Information Flyer, https://www.dtra.mil/Portals/61/Documents/DTRA_COVID_Final%2005112020.pdf?ver=2020-05-20-130911-847 (accessed August 13, 2020).
- 54 DTRA, *Basic Research for Countering Weapons of Mass Destruction*, 2010.
- 55 E. Chenoweth and S. E. Clarke, All terrorism is local: Resources, nested institutions, and governance for urban homeland security in the American federal system, *Political Research Quarterly*, 63 (2010): 495.

FEMA, Response, and Recovery

OBJECTIVES

1. To describe the early twentieth-century history of the Federal Emergency Management Agency (FEMA)
2. To outline the changes that FEMA underwent, both structural and policy oriented, between 1980 and 2015
3. To define the structural and policy changes that FEMA initiated as a result of the events of 9/11
4. To recognize the concept of preparedness and describe FEMA's philosophy, and the programs and policies that relate to it
5. To distinguish the various types of emergencies that exist—that is, natural disasters versus terrorist incidents and routine events versus catastrophic events—and their relative response differences
6. To comprehend the principle of mitigation in preparedness and outline the various FEMA programs that address mitigation
7. To understand the importance of post-assessment reports in preparedness, mitigation, response, and recovery planning
8. To distinguish the concepts of response and recovery and list the various initiatives undertaken by FEMA to make response timelier and more effective

7.1 Historical Foundation for FEMA

The pre-9/11 world was quite comfortable with the language of the protocol for disaster and its mitigation. From the 1930s onward, there were structural mechanisms to deal with disaster in the American landscape. The Reconstruction Finance Corporation provided loans for the repair and reconstruction of certain public facilities following disasters. The Bureau of Public Roads had the authority to fund the repairs of highways and bridges damaged by floods, earthquakes, and other disasters. In addition, the U.S. Army Corps of Engineers played an increasingly active role in the design of floodplains, levees, dams, and other edifices. In addition to the predictability of terror, and its use for pressing social and political change, it is expected that the federal

Homeland Security

government responds in times of emergency and disaster. It is a reasonable expectation that was sorely lacking in the Katrina debacle.

By the 1960s, it was evident that historic agencies were incapable of handling the larger natural disasters that plagued the country. It was clear that a major federal response and recovery agency was essential to serve those victimized by natural disaster. The Federal Disaster Assistance Administration, housed in Housing and Urban Development, was established. The National Flood Insurance program was set up in 1968, and executive orders and other presidential authority became a normative part of the disaster environment.

7.1.1 Federal Emergency Management Agency: Pre-9/11

In 1979, President Jimmy Carter, by executive order, merged a multitude of disaster agencies into FEMA. FEMA was to author an integrated emergency management system (IEMS) that covered “small isolated events to the ultimate emergency—war.” FEMA struggled to corral competing agency and bureaucratic interests and readily discovered the complexities of managing large- and small-scale disasters. Early in its operation, FEMA had to contend with

- Love Canal chemical disaster in Niagara Falls, New York
- Cuban boat refugee crisis
- Three Mile Island, Pennsylvania, nuclear plant crisis
- Hurricane Andrew
- Loma Prieta, California, earthquake

That FEMA adjusted its mission based on natural disasters and other environmental pressures is undeniable. FEMA was also continually reorganized in hopes that a centralized service would be a better brand of government response. For example, Reorganization Plan #3, adopted in 1978, integrated the National Fire Prevention Control Office, the Federal Broadcast System, the Defense Civil Preparedness Agency, the Federal Disaster Assistance Administration, and the Federal Preparedness Agency. Other inclusions in the latter part of the twentieth century were agencies that monitored earthquakes, dam safety, nuclear warning systems, and severe weather policy. In general, FEMA sought to implement an IEMS. In the early 1990s, FEMA’s capacity to respond to hurricanes and other natural disasters was severely tested, and “FEMA seemed incapable of carrying out the essential government function of emergency management.”¹

In its early life, FEMA’s philosophy of operation was narrower—in that it stressed the disaster side of emergency.

Internet Exercise: Read closely and consider the foundational laws that give FEMA legal authority for its many actions at <http://www.fema.gov/about-agency>.

That traditional definition, which includes flood, wind, earthquake, fire, and other natural disaster, tends to be distinctly different from the notion of terror. FEMA would eventually have to encompass terror—that intentionally inflicted disaster driven by an assortment of motivations. The Oklahoma City bombing of 1995 catapulted FEMA into the world of terrorist activity. Yet, the culture of FEMA, bound to the natural-disaster mentality, struggled to fit into the world of terror. At first, FEMA expended considerable energy urging communities to become disaster resistant and to erect mitigation policies that would prevent disasters of all sorts. Implementing *Project Impact: Building Disaster Resistant Communities* was the chief programmatic aim of FEMA in the late 1990s. In Project Impact, communities were to examine their communities in light of risk and adopt corresponding measures to mitigate the harm. FEMA’s central contribution during this period was to refocus communities, leaders, and the citizenry into the world of risk—natural or otherwise.

7.1.2 Federal Emergency Management Agency: Post-9/11

After the horrid events of 9/11, the mission of FEMA, its operational philosophy, and its ability to carry out its command were put to the test.² After 9/11, FEMA had to reorganize in two

ways: first, it had to continue its historic mission to deal with and respond to disaster; and second, it had to integrate a threat mentality as part of its obligation in serving the Department of Homeland Security (DHS). While natural disasters continue to be a crucial responsibility for FEMA, the world of terrorism increasingly dominates its outlook and mission. Hence, FEMA's mission is more encompassing than its historic expectation.

FEMA's mission is to support our citizens and first responders to ensure that as a nation we work together to build, sustain and improve our capability to prepare for, protect against, respond to, recover from and mitigate all hazards.³

Internet Exercise: Learn all about FEMA by reviewing the “We Are FEMA” video at <https://www.fema.gov/publ>

FEMA's merger has policy implications that it must adapt to. Figure 7.1⁴ charts the current structure of FEMA.

FEMA is led by an administrator and a whole host of deputy directors and administrators. FEMA also depends on the input and advice of its National Advisory Council, whose membership includes experts from both the public and the private sector. The National Advisory Council's input has been quite laudatory and more than pro forma comment. Since 2007, the council has directly dealt with many challenges but also with many success stories. The latest recommendations from their 2019 meeting deal with the public alert system.⁵ Other recommendations are:

Financial Preparedness

- Focus on Public Education
- Partner with Industry Groups to Maximize Impact

Closing the Insurance Gap

- Conduct Public Outreach Campaigns
- Increase Offerings of Parametric Insurance
- Stress Test State Insurance Guarantee Funds
- Use Emerging Technologies to Speed Payouts
- Reduce Self-Insurance for Public Infrastructure

Improving Code Adoption and Compliance

- Raise Awareness of the Consequences of Weak Codes
- Create Strong External Partnerships to Communicate the Importance of Codes
- Consider Requiring Building Codes and Building Code Compliance for FEMA Grant Programs, and Modernize NFIP Building Standards
- Provide a Self-Assessment Tool to Highlight the Benefits of Codes

Marginalized, Tribal, Rural, and Small Communities

- Simplify the THSGP Application Criteria
- Fund Tribal Nations in the Same Way Funds States Are Funded
- Reduce Enrollment Criteria for Local Delivery of Emergency Management Institute Courses in Rural Areas

Building Resilient Infrastructure in Communities

- Simplify the BRIC Scoring Criteria
- Expand the Definition of Eligible Projects
- Include Certain Small Projects That Cannot Be Approved with a BCA
- Develop a Toolbox to Support Stakeholder Mitigation Projects
- Allow Regular Use of Individual Economic Impact in All FEMA BCA Calculations

June 4, 2020

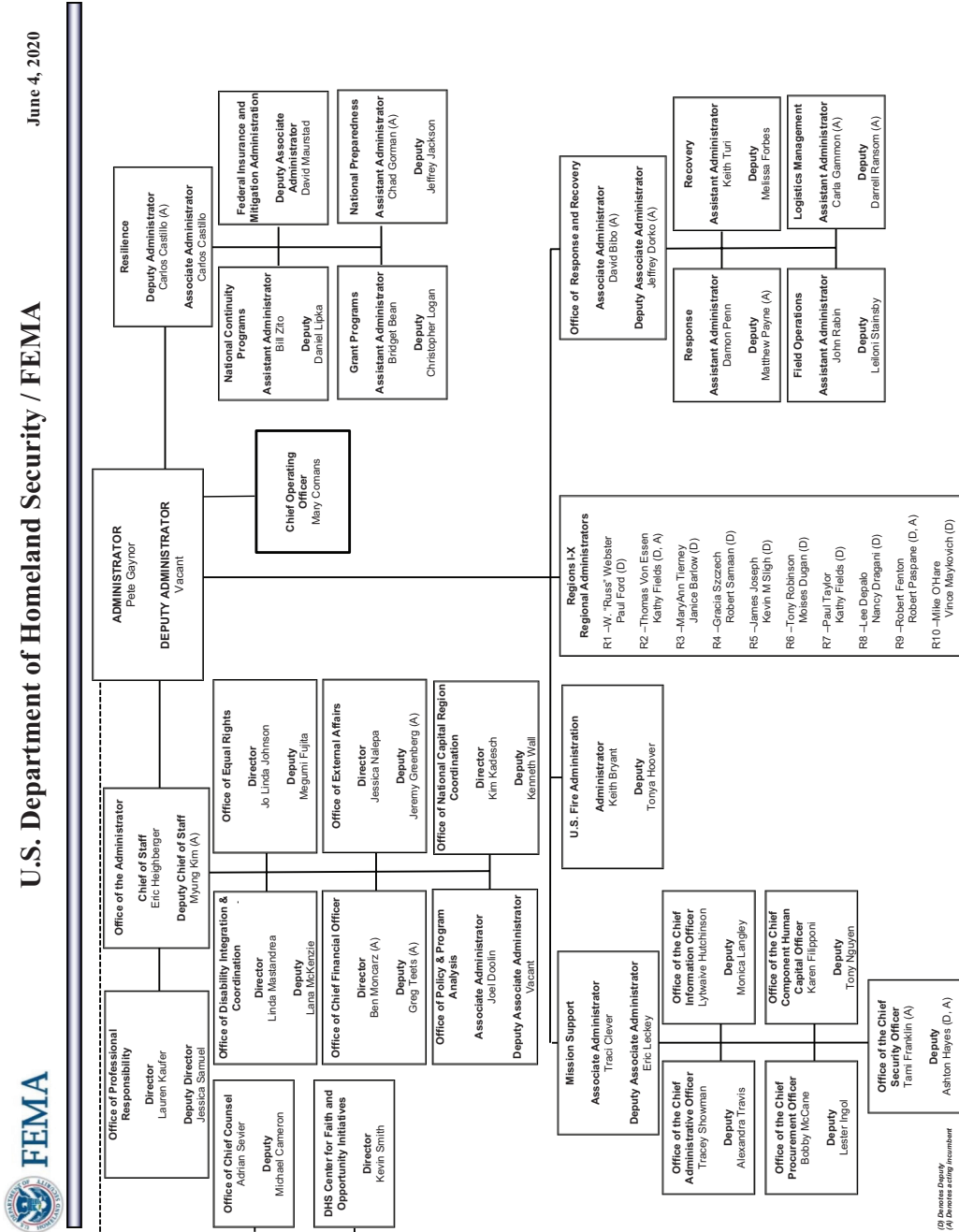


Figure 7.1 FEMA organization chart.

7.1 Historical Foundation for FEMA

- Encourage Cross-Jurisdiction Collaboration
- Seek Approval by Congress of Legislation to Encourage Cross-State Collaboration on Mitigation Projects
- Eliminate the Project Funding Cap
- Coordinate Funding Streams Across Federal Stakeholders
- Encourage Private Sector Investment
- Ensure Adequate Funding Is Set Aside for BRIC
- Eliminate the Project Funding Cap and Tie AA to Project Funding
- Require Use of Annually Updated Interest Rates in FEMA BCA Calculations

Immediate Needs Recommendations

- Amend Legal Authorities to Allow a STEP Version 2 Program in Jurisdictions with Mass Sheltering Needs (in Urban Areas)
- Establish a Consistent FIP Designation for NFIP Communities
- Review and Revise Current Flood Insurance Policy Correspondence and Practices
- Develop a Public Facing Mechanism for FIP Determinations⁶

Internet Exercise: Check out the membership roster of the current NAC at <https://www.fema.gov/national-advisory-council>.

Geographically, FEMA is further broken down into ten distinct regions to allow for greater local input and participation (see Figure 7.2).⁷

Finally, FEMA targets its subject matter by decentralizing into various *directorates*. These divisions provide the core, coordinated federal, operational, and logistical capability needed to save and sustain lives, minimize suffering, and protect property in a timely and effective manner in communities that become overwhelmed by natural disasters, acts of terrorism, or other emergencies. From assistance to mitigation, from logistics to the continuity programs, FEMA depends on its subject-matter specialists to deliver these services. The current directorates are

- Logistics management
- Response
- Recovery

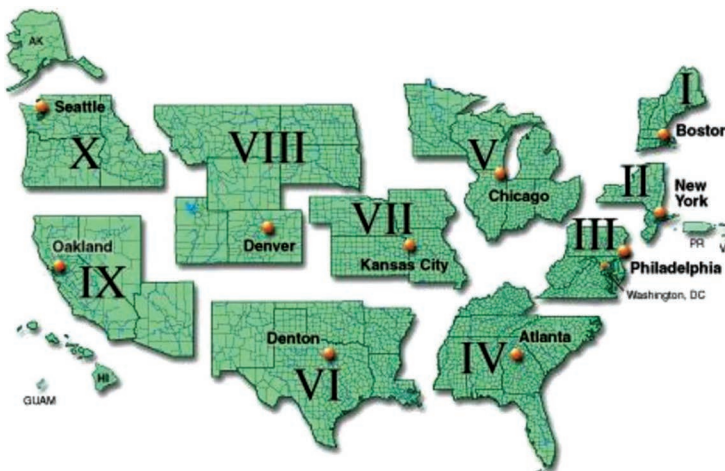


Figure 7.2 FEMA regions.

Homeland Security

- Field operations
- National continuity programs
- National preparedness
- Grant Programs

Internet Exercise: Read FEMA's strategic plan for the years 2018–2022 at https://www.fema.gov/media-library-data/1533052524696-b5137201a4614ade5e0129ef01cbf661/strat_plan.pdf

In its 2018–2022 Strategic Plan, FEMA has come, at least according to its critics, full circle, by finally recognizing its extraordinary complexity and bureaucratic pace. In the published Plan, the agency wants, in addition to other goals, to simplify and be more responsive. See Figure 7.3⁸ which posts FEMA's top three Goals in the years to come.



Figure 7.3 FEMA stated strategic goals.

There has been some debate recently as to what FEMA's role is during and in the wake of man-made and natural disasters, particularly in the area of recovery spending. Disasters present unique challenges according to the Center for Disaster Philanthropy:

The challenge...is that regardless of the size of the disaster, some affected individuals do not meet eligibility requirements for government disaster aid—and still others will have unmet needs even after receiving federal and/or state assistance. As FEMA Administrator Craig Fugate has said, “There’s no way government can solve the challenges of a disaster with a government-centric approach. It takes the whole team. And the private sector provides the bulk of the services every day in the community.”⁹

So, the questions arise: Where should the money for response and recovery come from? What criteria do disaster victims need to meet to be eligible for funds? Should taxpayers bear the cost of such funding? Is this a federal obligation or should it be a state and local issue? What role should the private sector play? Should those who pay for flood or hazard insurance be somehow rewarded for their advance planning while others are penalized?

Professor William Shughart II of the University of Mississippi sees those who have taken proper precautions—those who purchased insurance prior to the disaster event and understood the risks—as the party worthy of our protection and admiration. His argument is that this is good public policy that leads to a better, independent citizenry rather than individuals who are waiting for, and are dependent solely on, government assistance. According to Shughart:

People who voluntarily put themselves in harm's way, taking on the additional risks of living and working in disaster-prone areas, adequately insuring their lives and property against wind and flood—and paying actuarially fair premiums that reflect the greater risk—have every right to expect prompt reimbursement for the damages they sustained and every right to rebuild if they wish.¹⁰

As major disasters increase in scope, frequency, and damage costs—as has been the trend the last few decades—this debate as to who bears the cost of rebuilding and when to rebuild or not will certainly continue. Few would argue that COVID-19 Pandemic has stressed and strained our emergency system in ways never anticipated or envisioned.

7.2 FEMA and Preparedness

Any effective response, recovery, or other answer to a threat or catastrophe heavily depends on preparedness. By preparedness, one means that the agency, community, and constituency affected, as well as public and private partners, stand ready to deal with the threat in an effective manner.

Questions regarding the country's preparedness rose to the front and center after Hurricane Katrina. For the matter, those questions remain even in today's COVID-19 pandemic. And the questions seem endless:

- Why was the national stockpile not properly supplied?
- What was there shortages of PPE?
- Why were the states so ill-prepared for the pandemic?
- Why was there a shortfall of ventilators?

It is one thing to second guess during this pandemic, but quite another not to be properly prepared for the pandemic.

Internet Exercise: Visit the preparedness checklist at http://www.preparednessllc.com/assets/emergency_management_business_continuity_program_self-assessment-checklist.pdf

Various amendments to the *Homeland Security Act of 2002* established the National Preparedness Directorate (NPD). The directorate tackles many tasks in the area of preparedness, including

- Strategy, policy, and planning guidance to build prevention, protection, response, and recovery capabilities

Homeland Security

- Training courses, exercises, and technical assistance to ensure capabilities are standardized
- Coordination of FEMA regions as well as emergency management personnel at the federal, state, and local levels
- Coordination with other FEMA offices and directorates to produce a unified approach to emergency management

Running things at a national level is never an easy undertaking, and this challenge always adds to the difficulties. The Early Warning System—originally in color-coded formula—did not even have consensus as to what the colors meant nor did the colors really represent anything objectively accurate.¹¹ So subjective was the interpretation of the color-coded warning mode that emergency planners scrapped the system in 2013. In its place, emergency planners have come to depend on Emergency Alert System (EAS) participants who naturally communicate with others in the relevant geographic area. The EAS sends warnings via broadcast, cable, satellite, and wireline pathways. EAS participants, who consist of broadcast, cable, satellite, and wireline providers, are the stewards of this important public service in close partnership with alerting officials at all levels of government.

The EAS system is now labeled the Integrated Early Warning System (IPAWS), and under this system, officials at every level of government communicate with aligned agencies, other reporting authorities, and the public at large about impending harm or catastrophe.

Internet Exercise: See the IPAWS video on how it works at <https://www.fema.gov/media-library/assets/videos/77356>.

See Figure 7.4.¹²

Only approved public authorities may participate in the redesigned alert system used by FEMA. As of 2020,

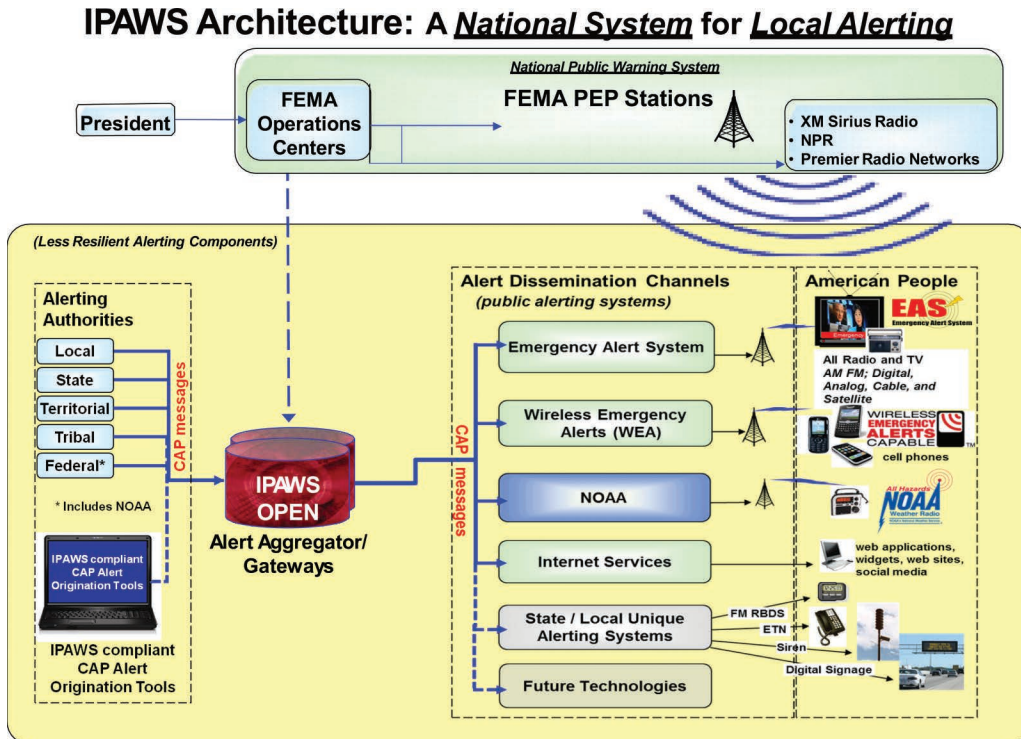


Figure 7.4 A diagram of the IPAWS architecture.

7.2 FEMA and Preparedness

there are more than 1,400 federal, state, local, tribal and territorial authorities that can use IPAWS to issue critical public alerts and warnings, and many more authorities that are in the process of obtaining the ability to issue alerts and warnings using IPAWS.¹³

Preparedness encompasses a whole range of operational and policy concerns for the homeland professional. Preparedness models envelop the capacity to plan, organize, train, equip, exercise, evaluate, and improve. FEMA charts the cycle of preparedness in Figure 7.5.

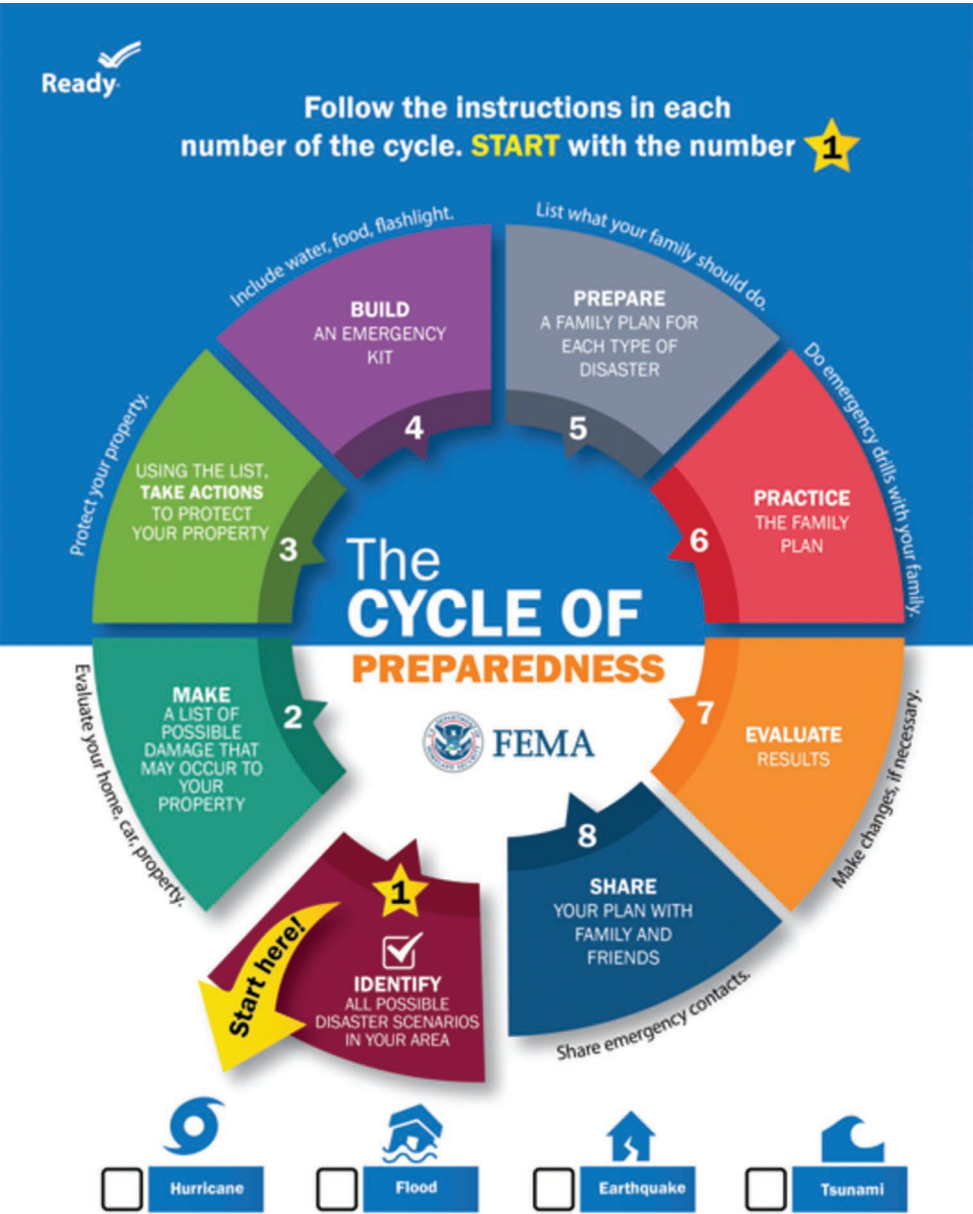


Figure 7.5 Preparedness cycle. Department of Homeland Security, *National Response Framework*, January 2008: 27, <https://www.fema.gov/media-library/assets/images/179379>.

Homeland Security

The catalogue of FEMA resources regarding preparedness is quite extensive. Already discussed in the text has been the citizen portal titled *Ready.gov* as well as the many functions and activities of the Citizen Corps. In addition to these resources, FEMA publishes a digital library—a searchable web-based collection of all publicly accessible FEMA information resources, including CDs, DVDs, VHS tapes, audiotapes, disability resources, posters and display items, brochures, publications, guidance and policy papers, program regulations and guidelines, forms, slide presentations, and other documents.¹⁴ The library is catalogued and organized in accordance with the hazard forms in Figure 7.6.¹⁵

If you are looking for:	Consider using:
Aftershock	Earthquake
Ash Fall	Volcano
Avalanche	Mudslide/Landslide, Winter Storm
Blizzard	Severe Storm, Winter Storm
Brush Fire	Wildfire
Cold	Extreme Temperatures, Winter Storm
Cyclone	Hurricane/Tropical Storm, Typhoon
Dust Storm	Drought, Extreme Temperatures, Severe Storm
Erosion	Coastal Storm, Hurricane/Tropical Storm, Typhoon
Explosion	Chemical/Biological, Fire, Nuclear, Technological, Terrorism
Flood, Flash Flood	Dam/Levee Break, Flooding
Forest Fire	Wildfire
Freeze	Extreme Temperatures, Winter Storm
Freezing Rain	Severe Storm, Winter Storm
Funnel Cloud	Tornado
Ground Saturation	Flooding
Hail	Severe Storm, Winter Storm

Figure 7.6 FEMA hazard forms cross-references.

(Continued)

If you are looking for:	Consider using:
Heat	Extreme Temperatures
High Surf	Coastal Storm, Hurricane/Tropical Storm, Tsunami, Typhoon
Ice	Extreme Temperatures, Winter Storm
Ice Jam	Flooding
Lava/Debris Flow	Volcano
Mold	Flooding
Power Outage	Technological, Terrorism
Radiological	Chemical/Biological, Nuclear, Terrorism
Rain	Flooding, Hurricane/Tropical Storm, Severe Storm, Typhoon, Winter Storm
Rock Slide	Mudslide/Landslide
Seismic Wave	Earthquake
Snow	Winter Storm
Snow Melt	Flooding
Storm Surge	Hurricane/Tropical Storm, Typhoon
Thunderstorm	Severe Storm
Tropical Depression	Hurricane/Tropical Storm, Severe Storm
Tidal Wave	Tsunami
Virus	Chemical/Biological, Terrorism
Wind	Coastal Storm, Hurricane/Tropical Storm, Severe Storm, Typhoon, Winter Storm
Waterspout	Tornado

Figure 7.6 (CONTINUED) FEMA hazard forms cross-references.

Homeland Security

FEMA orchestrates a narrower portal dedicated to natural disasters aptly titled *DisasterAssistance.gov*. The portal's primary aim is to assist those already harmed by natural disasters (see Figure 7.7).

The portal provides a wide array of services to those suffering from a multitude of disasters, but it also provides updated notices on current disaster declarations. See Figure 7.8¹⁶ for a list of the more recent disaster events.

Being prepared for radiological fallout from nuclear contamination is another FEMA responsibility. FEMA's Radiological Emergency Preparedness Program prepares for harm that may emerge in nuclear accidents and educates the public about this unique harm.¹⁷ Just as critically, FEMA plays a central preparedness role in the care, protection, and mitigation of chemical stockpiles across the continental United States. FEMA works in partnership with the United States Army to not only protect the stockpile but also to ensure the integrity of the same for the public at large. While stockpiles are slowly but assuredly being eliminated in the United States, there are nine locales across the nation for the storage of the same (see Figure 7.9 for current locations).



Georgia Avenue - Long Beach, New York

Figure 7.7 Before and after Hurricane Sandy: Georgia Avenue, Long Beach, NY, July 26, 2013. In November 2012, debris filled the streets as residents started to recover from the devastation of Hurricane Sandy. (www.dhs.gov.)

Disaster News Feeds

Get the latest information on declared disasters, storms and hurricanes and other recent natural disasters.

Recently Declared Disasters

No current disasters listed in the feed at this time.

Hurricanes

National Hurricane Center (NHS) Atlantic Map

- [The Atlantic hurricane season runs from June 1st through November 30th.](#)
- [Hurricane Lorenzo Graphics](#)

National Hurricane Center (NHC) Pacific Map

- [The Eastern North Pacific hurricane season runs from May 15th through November 30th.](#)
- [Eastern North Pacific Tropical Weather Outlook](#)
- [Remnants of Narda Graphics](#)

Earthquakes

- [M 5.7 - 25km SE of Saray, Turkey](#)
- [M 6.0 - 25km SE of Saray, Turkey](#)
- [M 7.7 - 123km NNW of Lucea, Jamaica](#)
- [M 7.0 - 93km ENE of Kuri'sk, Russia](#)
- [M 5.0 - 20km SSE of Guanica, Puerto Rico](#)

Severe Storms

- [SPC - No watches are valid as of Thu Feb 27 13:08:01 UTC 2020](#)
- [SPC Feb 27, 2020 1300 UTC Day 1 Convective Outlook](#)

Figure 7.8 DisasterAssistance.gov's website.

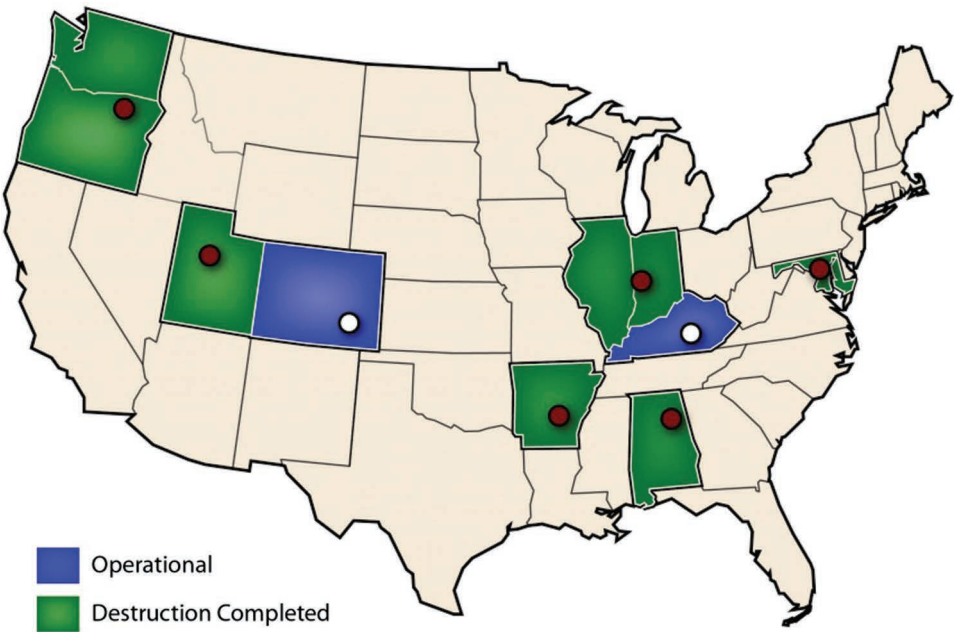


Figure 7.9 National chemical stockpile. The white dots indicate the last two operational stockpiles. The black dots are stockpiles that have been destroyed.

Homeland Security

Internet Exercise: Even individuals and families must be prepared for all eventualities. See the preparedness guide for chemical stockpile emergencies at https://www.fema.gov/media-library-data/1577991289556-ceaffbf3f4095b161e7364a2269659f1/2019_Program_Guidebook_FINAL.pdf.

Preparing the citizenry for hazard, disaster, and threat is a core mission of FEMA. Being ready—understanding the risk and taking preventive and mitigatory steps to minimize the damage—are the essential FEMA principles.¹⁸

How one goes about these functions largely depends on the type of threat or hazard under review.¹⁹ Floods and hurricanes are very different animals from nuclear leaks or sarin gas inhalation. The types of emergencies that occur daily, such as car accidents, road spills, or house fires, are routine events. Catastrophic events, such as tornadoes, terrorist attacks, superstorms such as Hurricane Sandy, or floods, tend to cover a larger area, impact a greater number of citizens, cost more to recover from, and occur less frequently.²⁰ See the table in Figure 7.10²¹ for event duration estimates.

The homeland specialist must first identify the risk and then take the necessary steps compatible with that risk. Some of the usual events are

- Dam failure
- Fire or wildfire
- Wildfire
- Hurricane
- Nuclear explosion
- Hazardous material
- Tornado
- Volcano
- Thunderstorm
- Earthquake
- Flood
- Winter storm

Classification	Routine		Catastrophic	
	Local	Regional	State	National
Examples	• Minor traffic incidents • Minor load spills • Vehicle fires • Minor train/bus accidents • Accidents with injuries but no fatalities	• Train derailment • Major bus/rail transit accidents • Major truck accidents • Multi-vehicle crashes • HazMat spills • Accidents with injuries and fatalities	• Train crashes • Airplane crashes • HazMat incidents • Multi-vehicle accidents • Tunnel fires • Multiple injuries and fatalities • Port/airport incidents • Large building fire or explosion • Industrial incidents • Major tunnel/bridge closure	• Terrorist attack/WMD • Floods, blizzards, tornadoes • Transportation infrastructure collapse • Extended power/water outages • Riots • Mass casualties
Expected event duration	0–2 Hours	2–24 Hours	Day	Weeks

Figure 7.10 Duration estimates for catastrophic and routine emergency events.

- Landslide
- Terrorism
- Heat
- Tsunami

FEMA uses high-level technology to estimate and predict damage and potential harm. It has developed comprehensive software programs that are crucial to predicting the outcomes of particular events (Figure 7.11).

Hazus is a product that uses current scientific and engineering knowledge, coupled with the latest geographic information systems (GIS) technology, to produce estimates of hazard-related damage before, or after, a disaster occurs. Depending on the threat or harm, Hazus will evaluate and estimate losses after inputting criteria. The Hazus software program assesses risk in a five-step process, as outlined in Figure 7.12.²²

Hence, preparedness steps will largely depend on the threat. While Hazus works in natural disasters, its effectiveness in terror is less predictable and useful.²³ To close the knowledge gap on the national level, FEMA sponsors annual Hazus conferences, which have included specialized training in flood mitigation, cost-benefit analysis, storm surge, and other coastal threats.

Internet Exercise: Discover Hazus success stories at <https://www.fema.gov/hazus>.

Be mindful that software updates are going to be regular occurrences in the Hazus market. FEMA just released Hazus 3.0, and another edition can be expected in another year or so.²⁴

Since Katrina, FEMA has evolved in mostly beneficial ways for many of its responses. Katrina was a wakeup call about the concept of preparedness—being able to respond with professionalism and efficacy. Since Katrina, the agency has been bombarded with a legion of natural disasters and can mostly hold its head high in its handling of these many events. “FEMA gets high marks from disaster experts for inserting field staff into the disaster zone quickly and opening up communication with local and state officials.”²⁵ Some have even argued that during the last decade, especially since Katrina, the agency is now in the “groove.”²⁶ The advance warning notification and response, in large part, to Hurricane Sandy is a direct reflection of some of the

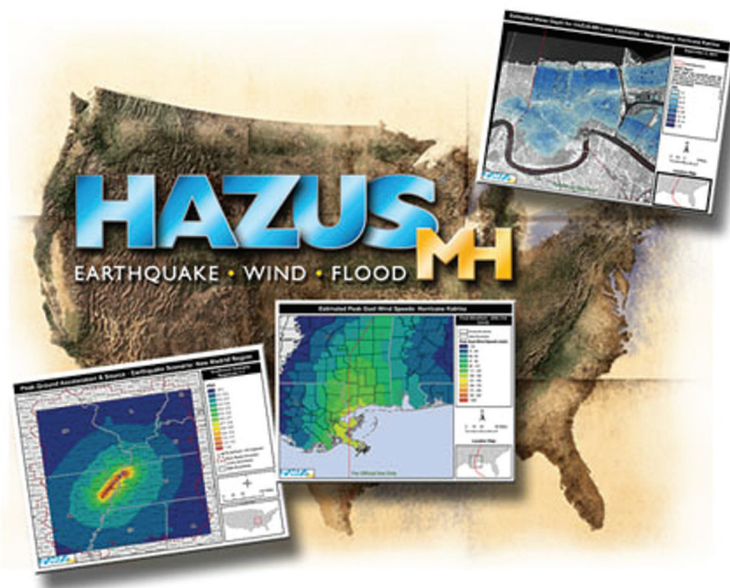


Figure 7.11 The Hazus-MH data extractor is a tool for extracting data from Hazus-MH data sources.

Homeland Security

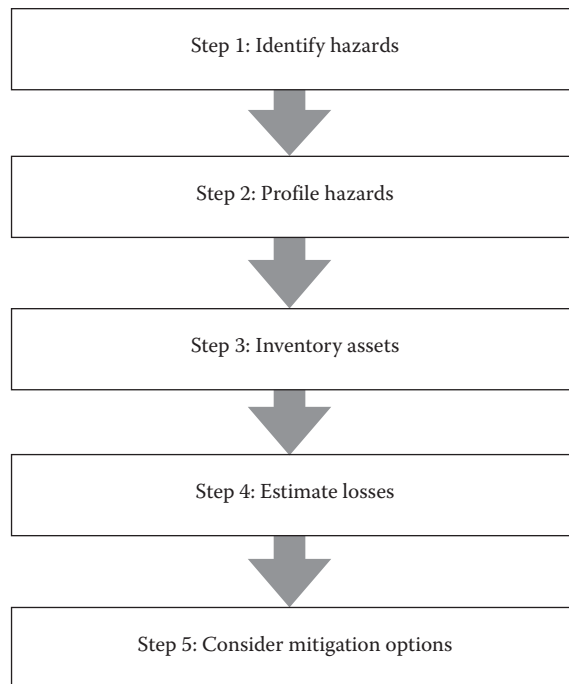


Figure 7.12 Hazus process flowchart.

positive changes, particularly under Administrator Craig Fugate, who has headed up FEMA since 2009. FEMA has most helpfully prepared a series of Risk Management Guides on a host of location and facilities. A summary list is reproduced below.

- FEMA 426/BIPS 06—Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, 2nd Edition (2011)
- FEMA 427—Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks (2003)
- FEMA 428/BIPS 07—Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings, 2nd Edition (2012)
- FEMA 429—Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings (2003)
- FEMA 430—Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks (2007)
- FEMA 452—A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings (2005)
- FEMA 453—Safe Rooms and Shelters: Protecting People Against Terrorist Attacks (2006)
- FEMA 455—Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks (2009)
- FEMA 459—Incremental Protection for Existing Commercial Buildings from Terrorist Attack: Providing Protection to People and Buildings (2008)²⁷

7.2.1 Role of Mitigation in the Preparedness Model

Once the threat has been identified and the inventory or potential costs calculated, the homeland professional seeks ways to mitigate the harm. The term *mitigation* implies an intervention before the threat or catastrophe takes place. Mitigation is the effort to reduce the loss of life and property by lessening the impact of disasters. Effective mitigation measures can break the cycle of disaster damage, reconstruction, and repeated damage. While it cannot work in all homeland threats, the idea of mitigation works particularly well in the case of natural disasters, fire, and other catastrophes. For example, in the event of a hurricane or flood or even a nuclear attack, there are mitigation steps that may prevent the level of expected destruction. Building design, for instance, goes a long way to mitigate the impact of either the earthquake or the flood. Hence, FEMA encourages a variety of mitigation programs to minimize and limit damage and threat. Particular attention is given to the mitigation of buildings against terrorist threat and the security and safety of schools, hospitals, and government installations (see Figure 7.13).²⁸

What is the Risk Management Series?

The Risk Management Series (RMS) is a new FEMA series directed at providing design guidance for mitigating multihazard events. The objective of the series is to reduce physical damage to structural and nonstructural components of buildings and related infrastructure, and to reduce resultant casualties during natural and manmade disasters.

The RMS is intended to minimize conflicts that may arise from a multihazard design approach. A multihazard approach requires a complex series of tradeoffs. Security concerns need to be balanced with requirements in terms of earthquakes, floods, high speed winds, accessibility, fire protection, and aesthetics, among others. Designing to mitigate natural hazards should avoid considering manmade hazards as an afterthought, but rather as a critical concern to be studied early during the project cycle. Natural hazards are the largest single contributor to catastrophic or repetitive damage to communities nationwide. Manmade hazards can be categorized as rare events with a potential high impact and very difficult to predict.



Risk Management Series

Minimizing the Effects of Natural Disasters and Potential Terrorist Attacks on Large Buildings



FEMA

Figure 7.13 FEMA's risk management series.

Homeland Security

Congress has repeatedly increased the funding for mitigation programs, since it is now self-evident that mitigation is quantifiably demonstrable. Mitigation programs have “demonstrated cost reductions following disasters due earlier mitigation investments.”²⁹ What is just as deducible is that mitigation plans lack a universality and national design with states and localities treating some portion of the total variable relevant in a mitigation program. For example, the pre-mitigation analysis must consider evacuation as a legitimate part of the mitigation program. If one does not account for the means, the methods, or the alternatives in evacuation, aside from being caught flat-footed, the expense of failing to plan will surely be higher than the expense of being organized. Drs. Olornilua and Ibitaya surprisingly conclude that this lack of uniformity directly undermines our planned efficiencies and that every mitigation plan must prepare for “multi-hazard” situations. The lack of uniformity is portrayed as “dismal.”³⁰

In the area of earthquakes, FEMA sponsors the National Earthquake Hazards Reduction Plan (NEHRP) (Figure 7.14).

Its primary goals are to

- Develop effective practices and policies for earthquake loss reduction and to accelerate implementation
- Improve techniques to reduce the seismic vulnerability of facilities and systems
- Improve seismic hazards identification and risk assessment methods
- Improve the understanding of earthquakes

National Earthquake Hazards Reduction Program

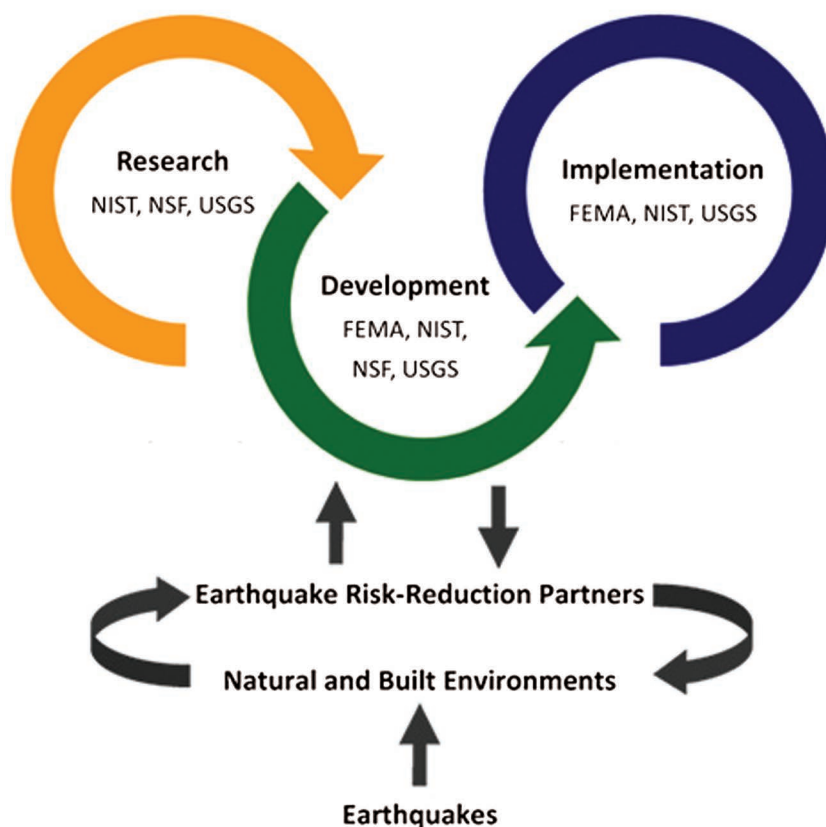


Figure 7.14 National Earthquake Hazards Reduction Plan process chart.

In earthquake design, the building must be capable of withstanding the move and sway caused by the earthquake. The recent completion of the Paramount, a high-rise office complex in San Francisco, an earthquake-prone area, manifests the role of engineering design in building plans. In the Paramount, precast concrete is utilized as well as the Precast Hybrid Movement Resistant Frame (PHMRF) system (Figure 7.15).

These same mitigation principles apply to a host of other settings, including dams and waterways. FEMA's National Dam Safety Program (NDSP) identifies, develops, and enhances technology to track the condition of the dam infrastructure. FEMA hosts the following initiatives:

- *National Inventory of Dams*: A computerized database of U.S. dams.
- *National Dam Safety Program management tools*: An information collection and management system used by federal and state dam safety program managers.
- *National Performance of Dams Program*: A national effort headquartered at Stanford University that tracks dam performance.

Internet Exercise: Read the biennial report of the National Dam Safety Program at <https://www.fema.gov/media-library-data/1470749866373-5de9234b8a02a3577c2646ffdf6eb087/FEMAP1067.pdf>.

The preparedness and mitigation stress continue into the world of hurricanes. FEMA, in collaboration with a host of other agencies, such as the National Oceanic and Atmospheric Association, National Weather Service, U.S. Department of Transportation, and U.S. Army Corps of Engineers, is deeply involved in the preparation and planning for and the mitigation of hurricanes. Some activities include:

- Planning for safe and effective evacuations
- National Hurricane Program (NHP) training
- Response and recovery



Figure 7.15 The Paramount building in San Francisco. (Courtesy of FEMA.)

Homeland Security

- Post-storm assessments
- Mitigation as to hurricane losses

Established in 1985, the NHP conducts assessments and provides tools and technical assistance to assist state and local agencies in developing hurricane evacuation plans. Aside from planning, preparedness, and mitigation, FEMA, by and through the NHP, relies on a Hurricane Liaison Team (HLT) that coordinates the various levels of government response as well as private-sector players. HLT members provide critical storm information to government agency decision makers at all levels to help them prepare for their response operations, which may include evacuations, sheltering, and mobilizing equipment. The HLT works closely with states and localities.³¹

FEMA also relies on Mitigation Assessment Teams (MATs), which it assigns to vulnerable areas. MATs see the real and meaningful impact of natural disasters and the steps that could have eliminated some of the losses. The MAT will

- Assess the vulnerability of buildings
- Increase building resistance to damage caused by hazard events

MATs look closely at building codes and standards, designs, methods, and materials used for new construction and post-disaster repair and recovery.

Internet Exercise: Find out about careers in MATs and the current recruitment efforts by FEMA at <https://www.fema.gov/emergency-managers/risk-management/building-science/mitigation-assessment-team>.

Flood threats are a continual concern for the FEMA mission and its operational personnel. The last decade has witnessed a wave of flood events caused by anything from heavy rains to hurricanes. This includes areas that are regularly prone to reoccurrences of disaster-level flooding. Critics, and even the independent government Congressional Research Service, have questioned the efficacy of the National Flood Insurance Program (NFIP), originally established in 1968 as a measure to “address the nation’s flood exposure and challenges inherent in financing and managing flood risks in the private sector.”³²

DHS even publishes a list of repeat and very expensive performers in the world of floods (see Table 7.1³³).

Homebuilders are now required to anticipate the reality of flood when designing residential and commercial buildings. Gone are the days when design could disregard the elements.

FEMA publishes how-to guides for construction companies so that damage may be mitigated. Figure 7.16³⁴ portrays the need for a stainless-steel house wrap that minimizes water damage.

Internet Exercise: Read the FEMA construction advice on building in flood-prone areas at <https://www.fema.gov/emergency-managers/practitioners/case-study-library>.

So important is the minimization of flood damage before the flood occurs that FEMA has erected a subagency—the Federal Insurance and Mitigation Administration (FIMA)—solely dedicated to flood mitigation. Mitigation steps directly minimize the extraordinary economic losses that are part of the damage analysis. Whole neighborhood, streets, and commercial districts are impacted severely by flood damage. The 2020 Hurricane Michael brought havoc to many communities in the South. How to minimize this level of damage is a FIMA and FEMA function.³⁵

The power and might of flood damage are evident in not only singular homes but entire communities especially those built before newly adopted standards of elevated structures were adopted in the early 2000s. See Figure 7.17 for an entire parcel of the community destroyed by flood damage in Mexico Beach, Florida.

FIMA deals with:

- Complying with or exceeding NFIP floodplain management regulations
- Enforcing stringent building codes, flood-proofing requirements, seismic design standards, and wind-bracing requirements for new construction or repairing existing buildings

Table 7.1 Top 15 Significant Flood Events Covered by the National Flood Insurance Program				
Event	Year	# PD Losses	Amount PD (\$)	AVG PD Loss
Late Winter Severe Storms	Mar-16	5,318	\$283,711,582	\$53,349
Late-Spring Storms	Jun-11	2,435	\$134,795,849	\$55,358
Torrential Rain – Tn	Apr-10	4,119	\$230,583,017	\$55,980
Hurricane Ivan	Sep-04	28,154	\$1,607,512,533	\$57,097
Hurricane Michael	Oct-18	3,490	\$201,562,277	\$57,754
Hurricane Ike	Sep-08	46,701	\$2,702,388,727	\$57,866
Hurricane Maria	Sep-17	640	\$38,050,370	\$59,454
Torrential Rain Sept 2009 Ga	Sep-09	2,068	\$124,448,580	\$60,178
Torrential Rain – Texas	Apr-16	7,437	\$471,517,374	\$63,402
Superstorm Sandy	Oct-12	132,360	\$8,804,242,152	\$66,517
Texas Flooding May Jun 2015	May-15	6,774	\$468,799,696	\$69,206
Louisiana Severe Storms and Flooding	Aug-16	26,976	\$2,468,493,541	\$91,507
Hurricane Katrina	Aug-05	166,790	\$16,257,744,061	\$97,474
Hurricane Harvey	Sep-17	76,257	\$8,908,547,689	\$116,823

Source: U.S. Department of Homeland Security, Federal Emergency Management Agency.

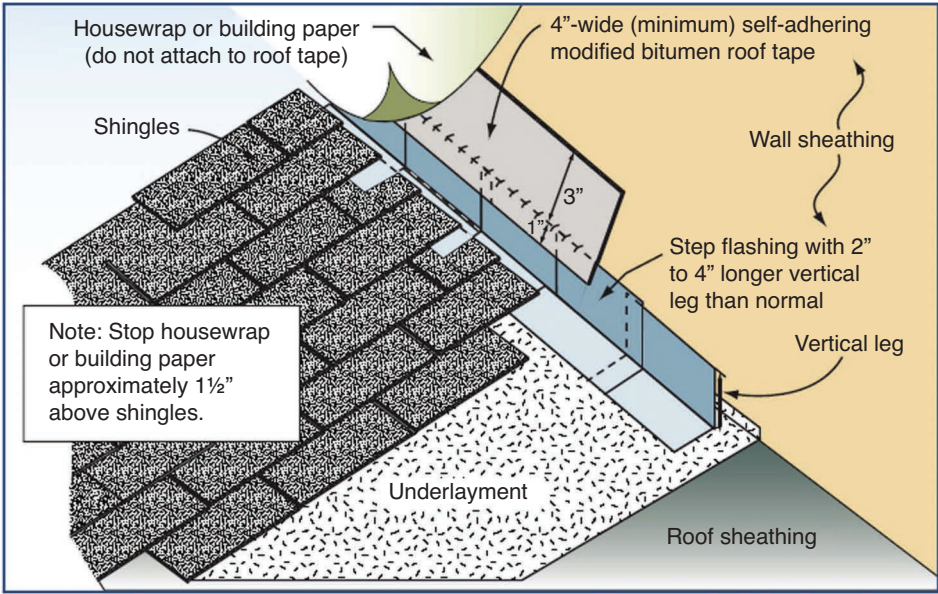


Figure 7.16 FEMA construction guidelines to help mitigate roof damage.

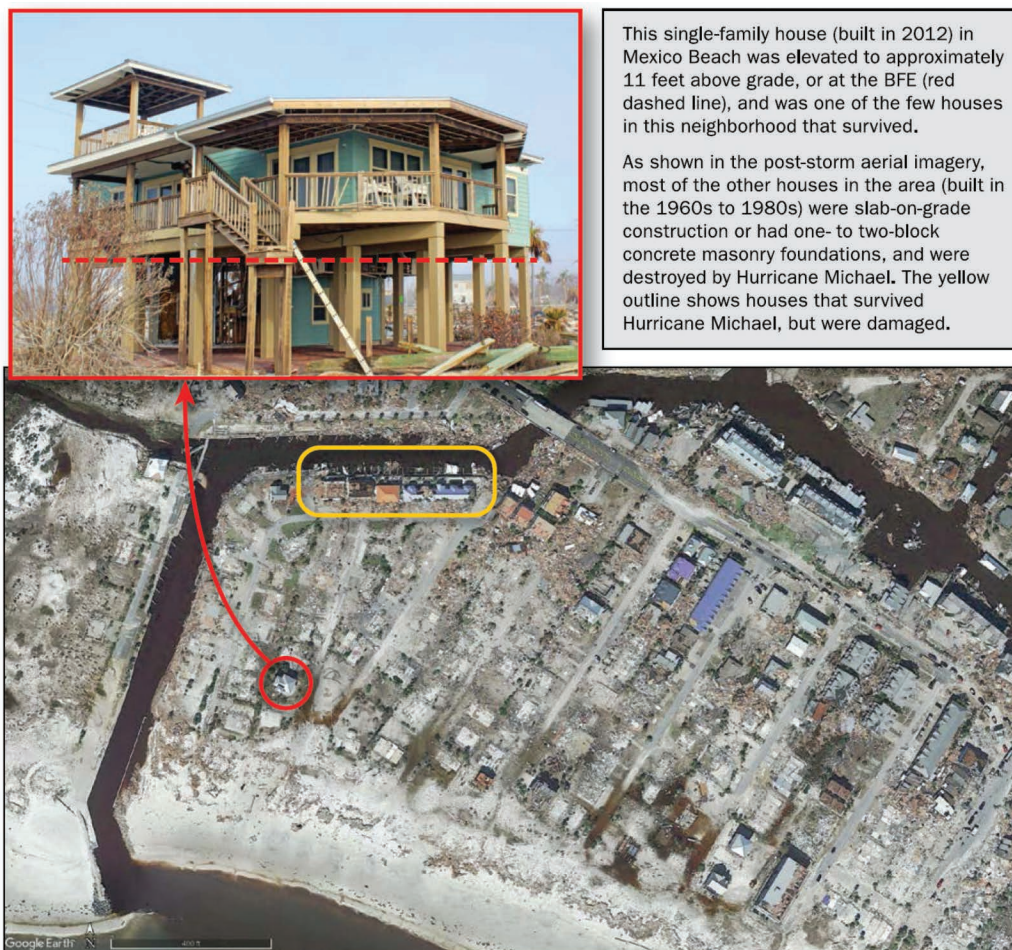


Figure 7.17 Post-storm aerial image of a beachfront residential community in Mexico Beach that was heavily damaged by both wind and flood during Hurricane Michael (Mexico Beach; Zone VE, Zone AE, and unshaded Zone X).

7.2 FEMA and Preparedness

- Adopting zoning ordinances that steer development away from areas subject to flooding, storm surge, or coastal erosion
- Retrofitting public buildings to withstand hurricane-strength winds or ground shaking
- Acquiring damaged homes or businesses in flood-prone areas, relocating the structures, and returning the property to open space, wetlands, or recreational uses
- Building community shelters and tornado safe rooms to help protect people in their homes, public buildings, and schools in hurricane- and tornado-prone areas

In the area of risk assessment, FEMA has instituted a wide array of programs, including:

- Flood hazard mapping
- Hazus-MH—the software program for disasters
- Mitigation planning—the full body of steps to minimize damage

In mapping, FEMA has made its greatest contribution. In the FEMA Flood Map Service Center, professionals can scan and assess just about every geographic area prone to flooding. FEMA's new MAP MOD program is an ambitious attempt to draw the flood-prone areas. Using the latest mapping technology, including but not limited to GIS-based format, flood maps are now digitally produced.

Internet Exercise: Find out your neighborhood's flood potential by visiting the FEMA map center at <http://msc.fema.gov/portal>.

On top of these plans, the Agency has created toolkits for individuals and businesses for diverse disasters.³⁶ See Figure 7.18.³⁷

Risk reduction weighs on FEMA policymakers daily, for if there is any truism about floods and other natural disasters, it is that these events will reoccur. FEMA expends significant energy educating the public about floods and how to prepare.³⁸ For example, FEMA's FloodSmart



Figure 7.18 The Ready Business Hurricane Toolkit.

program³⁹ provides a significant array of tools and resources to the homeowner. Figure 7.19 summarizes these options concerning the important role of flood insurance in time of disaster.⁴⁰

Internet Exercise: Use the NFIP cost calculator regarding flood damage at <https://www.floodsmart.gov/flood-insurance-cost/calculator>



FloodSmart Online Tools and Resources

FloodSmart—the marketing campaign for the National Flood Insurance Program (NFIP)—provides an array of tools and resources that help educate people about their flood risk and how they can financially protect themselves with flood insurance. The tools are available on the FloodSmart website, [FloodSmart.gov/partnertools](https://www.floodsmart.gov/partnertools). FloodSmart makes these and other resources available for community officials, insurance agents, floodplain managers, and other stakeholders to download and use in their own outreach.

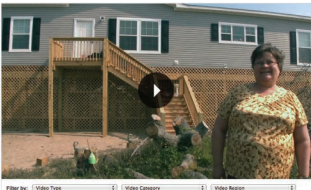


The Starting Point: FloodSmart.gov

FloodSmart.gov is the official website of the NFIP, where users can determine their property's flood risk, learn about flood insurance, and discover ways to reduce their risk. The site also offers a wealth of downloadable materials and shareable tools. Click [Community Resources](#) on the [FloodSmart.gov](https://www.floodsmart.gov) home page to find ready-to-use videos, fact sheets, Web banners, widgets, and more. FloodSmart encourages emergency management agencies, state and local officials, and other stakeholders to offer links to [FloodSmart.gov](https://www.floodsmart.gov) in their communications and to feature the resources, tools, and widgets on their own sites. Resources include:

Video Testimonials

These are compelling videos of home and business owners sharing first-hand accounts of their experiences with floods caused by coastal storms, levee breaches, seasonal rains, and hurricanes. Use them in presentations or link to them from your website. View or link to the testimonials at [FloodSmart.gov/testimonials](https://www.floodsmart.gov/testimonials). Obtain copies by emailing info@fema-floodsmart.com.

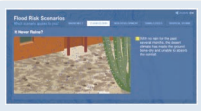


Interactive Tools You Can Use

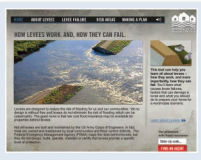
FloodSmart has built interactive tools that illustrate the causes of flooding, the costs of flooding, and how living behind a levee increases your risk of flooding. Coming soon: a coastal flood simulator! FloodSmart makes the embed code available so you can post the tools to your community's website.



Cost of Flooding: Users of this interactive tool choose how deep the flood waters could be in a home. The tool then itemizes what could be damaged and what the final cost might be to replace damaged items. It is an excellent way to illustrate the financial consequences of a flood.



Risk Scenarios: These simulations illustrate common factors that affect flood risk including snow melt, flash flooding, new development, dams, levees, and tropical storms. Users can click on the scenarios to see examples of how and why it can flood.



Levee Simulator: This tool helps explain how levees work and how they can fail. Users see simulations of what causes levee breaches, seepage, and overtopping as well as photos and videos of real-life examples.



MARCH 2013

Figure 7.19 FEMA's FloodSmart Program—Educate Yourself.

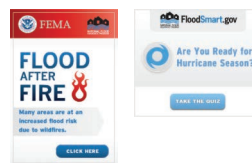
(Continued)

Widgets

These short informational simulations don't take up much room on your website, but they capture attention and direct visitors to more detailed information. Each year, FloodSmart creates and updates widgets that can help educate people about the risk of flooding. For example, seasonal widgets are available for flood after fire and hurricane season. These widgets easily can be downloaded from the [Community Resources](#) page on [FloodSmart.gov](#).

Toolkits

FloodSmart's [Flood Outreach](#) toolkit includes fact sheets, messaging, outreach planning support, and other information that emergency managers and other stakeholders can use to address flood risks and promote flood insurance. The [mapping](#) and [levee](#) toolkits help to communicate changes in flood hazard maps and teach communities about levee issues through outreach material and letter templates ready for you to customize.



The risk of flooding is real. Together we can help residents and business owners better understand the risk of flooding and take action to lessen the financial consequences. These tools and resources help bring the story home and make it more personal. Don't wait to use them. Visit [FloodSmart.gov](#) and start right away. For more information, contact FloodSmart at info@fema-floodsmart.com.

Figure 7.19 (CONTINUED) FEMA's FloodSmart Program—Educate Yourself.

Aside from its educational role, FEMA promotes a host of other risk reductions, including its National Flood Insurance Program, its flood map center, and its software programs for both individual and commercial interests. Additionally, FEMA has devised a repetitive loss program according to which flood-prone areas must implement mitigation steps to thwart the ensuing damages. See Figure 7.20 for the cover page relating to repetitive loss.

FEMA provides grants and other financial support to implement mitigation plans. To spend money now to avoid future catastrophic costs, evidences sound policy. Just as compellingly, FEMA serves as a depository for best practices in the world of catastrophic mitigation. By best practices, we mean a collection of what in fact works in the event of flood or other hazard or threat. FEMA labels the most effective mitigation practices as either superior or commendable. FEMA publishes a compendium of exemplary or best practices in the area of mitigation and preparedness. It asks practitioners in the homeland security field to submit programs that they consider not only workable but on the cutting edge of innovation in mitigation. FEMA defines an exemplary program as

an exemplary practice in emergency management is any practice, project, program, technique, or method that works in one place and is worthy of copying and can be copied elsewhere. It includes initiatives such as inventive coordination among organizations, volunteer projects and resource sharing, and other innovative and highly effective emergency management activities.⁴¹

Finally, FEMA relies on agencies to conduct post-assessment reports after the hurricane has passed. Post-assessment reports are essential for FEMA's future operations since these documents provide lessons learned from past storms; measures of hurricane and coastal flooding preparedness; the need for reform in public policy, building performance, and hurricane mitigation; the assessment of growth and the efficacy of evacuation shelter selection guidelines; and other contingency planning. FEMA also needs to determine where it can be more efficient

Homeland Security

and cost conscious. With rising economic challenges, the agency must carry out its functions with fewer funds and fewer people. In the age of smartphones and mobile communications, the agency must incorporate more innovative technology when communicating with its constituencies.⁴² As a result, FEMA must aggressively employ all forms of social media to get the warning

Federal Emergency Management Agency National Flood Insurance Program

OMB 1660-0022 EXPIRES August 31, 2010

NFIP REPETITIVE LOSS (RL) UPDATE WORKSHEET (AW-501)

NOTE: SEE REVERSE SIDE FOR MITIGATION ACTION CODES AND PAPERWORK BURDEN STATEMENT

Printed On:

THE INFORMATION ON THIS FORM IS BASED ON CLAIMS ON OR BEFORE:

REPETITIVE LOSS NUMBER:

Internal use only ☐ A ☐ N/A ☐ FRR	
CURRENT NFIP COMMUNITY NAME:	
COMMUNITY ID #:	
CURRENT PROPERTY ADDRESS	PREVIOUS PROPERTY ADDRESS/COMMUNITY ID #
LAST CLAIMANT:	
INSURED: NAMED INSURED:	
DATES OF LOSSES TOTAL NUMBER OF LOSSES FOR PROPERTY:	

REQUESTED UPDATES

MARK ALL UPDATES BELOW THAT APPLY (IMPORTANT – READ THE INSTRUCTIONS)

1. ☐ INFORMATION PROVIDED NOT SUFFICIENT TO IDENTIFY PROPERTY.
Choose this update if all attempts to locate the property fail. Please describe the steps you took to locate the property in the comments section below.
2. ☐ COSMETIC CHANGES REQUIRED TO THE ADDRESS:
Use this update to correct or update the property address shown above.
Only change the address not the name.
3. ☐ PROPERTY NOT IN OUR COMMUNITY OR JURISDICTION:
Choose this update if you have positively determined that the property shown is not located in your community. Please provide the correct community name and if known the NFIP Community ID Number. If available, please attach a map showing the property location.
- ASSIGN TO COMMUNITY NAME: _____ NFIP COMMUNITY ID # _____
4. ☐ FLOOD PROTECTION PROVIDED.
Choose this update only if some type of structural intervention has occurred to the building, property or the source of flooding that protects the building from future events similar to those that occurred in the past. The correction must be supported by documentation such as an Elevation Certificate and the Mitigation information below must be provided.
- Mitigation Action 1.) ☐ Source of Mitigation Funding 3.) ☐ See the back of this form for the appropriate codes.
5. ☐ NO BUILDING ON PROPERTY.
Choose this update only if the property in question can be positively identified as the site of the previously flooded building and documentation is available to support that an insurable building no longer exists at this site. The correction must be supported by documentation such as a Demolition or Relocation Permit and the Mitigation information below must be provided.
- Mitigation Action 2.) ☐ Source of Mitigation Funding 3.) ☐ See the back of this form for the appropriate codes.
6. ☐ DUPLICATE LISTING WITH RL NUMBER: _____ COMBINE AS ONE LISTING.
Choose this update to identify two or more separate listings that are for the same building. List all other RL numbers that are duplicates to this property. Please indicate which address shown is the correct address to use.
7. ☐ HISTORIC BUILDING: Check this box if you know the building is listed on a State or National Historic Registry.

ADDITIONAL COMMENTS: _____

A SIGNED RL TRANSMITTAL SHEET MUST ACCOMPANY THIS FORM FOR APPROVAL OF THE UPDATE!

SEE PRIVACY ACT STATEMENT ON THE BACK

Figure 7.20 Repetitive loss update worksheet.

(Continued)

MITIGATION ACTION CODES

- 1.) If you checked the box that says "FLOOD PROTECTION PROVIDED," please enter the letter below (a –f) that best describes the situation:
- a. The building was elevated to or above the Base Flood Elevation (BFE).
 - b. The building was elevated but not to the BFE.
 - c. The building (non-residential) was floodproofed to the BFE.
 - d. The building was partially floodproofed (but, not to the BFE).
 - e. The building was protected by a flood control/stormwater management project.
 - f. The building was replaced by a new elevated/floodproofed building.
- 2.) If you checked the box that says "NO BUILDING ON PROPERTY," please enter the letter below (g – i) that best describes the situation.
- g. The building was demolished, but not acquired through any program.
 - h. The building was acquired and demolished as part of a program.
 - i. The building was relocated out of the floodplain.

MITIGATION FUNDING CODES

- 3.) Please choose from the following (j – y) to identify the primary and secondary funding sources for the mitigation action described by a – i above.

FEMA PROGRAMS	NON FEMA FUNDING SOURCES
j. Hazard Mitigation Grant Program (HMGP).	q. Increased Cost of Compliance (ICC) coverage.
k. Flood Mitigation Assistance Program (FMA).	r. U.S. Housing & Urban Development (HUD) Community Development Block Grant (CDBG).
l. Pre-Disaster Mitigation Grant Program (PDM).	s. U.S. Army Corps of Engineers or Natural Resources Conservation Service (NRCS) Project.
m. Repetitive Flood Claims (RFC)	t. Other Federal Program.
n. Severe Repetitive Loss Program (SRL)	u. State Program.
o. Section 1362 Acquisition Program.	v. Local Program.
p. Other FEMA Programs	w. Property Owner
	x. Natural Disaster or Fire.
	y. Unknown

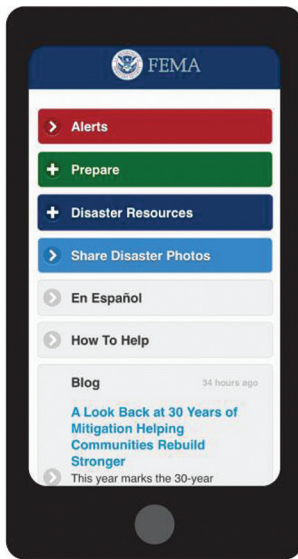
OMB Statement: Public reporting burden for this information collection is estimated at 35 hours for the application and certification process. Burden means the time, effort and financial resources expended by persons to generate, maintain, retain, disclose, or to provide information to us. You may send comments regarding the burden estimate or any aspect of the collection, including suggestions for reducing the burden to: Information Collections Management, U.S. Department of Homeland Security, Emergency Preparedness and Response Directorate, Federal Emergency Management Agency, 500 C Street, SW, Washington, DC 20472, Paperwork Reduction Project (OMB Control Number 1660-0022). You are not required to respond to this collection of information unless a valid OMB control number appears in the upper right corner of this form. Note: Do not send your completed questionnaire to this address.

Privacy Act: The information contained in this transmittal is legally privileged and confidential. Its use is protected under the Privacy Act of 1974, 5 U.S.C. Section 552(a). Use of the provided information is restricted to the applicable Routine Use(s) cited in the System Notice published at 67 FR 3193 January 23, 2003. The information provided should be used consistently with the purpose(s) for which the records were released as stated in the applicable Routine Use(s) cited herein.

Further, under the Privacy Act of 1974, 5 U.S.C. Section 552(a), personal identifiers, such as names, may be used only for limited purposes. One of the allowable uses of names and flood insurance claims history is to analyze the effectiveness of local flood loss reduction efforts. In addition, the Routine Use furthers the floodplain management and hazard mitigation goals of the Agency by making more detailed NFIP records available to communities. Communities may use personal identifiers for this purpose only and are prohibited from using them for solicitation, or other reasons.

Figure 7.20 (CONTINUED) Repetitive loss update worksheet.

Homeland Security



Receive **real-time alerts** from the National Weather Service for up to five locations nationwide.



Learn **emergency safety tips** for over 20 types of disasters, including earthquakes, fires, hurricanes, tornadoes and more.



Locate open **emergency shelters** in your area and find **disaster recovery centers** where you can talk to FEMA in person.



Share alerts via text, email and social media.

Figure 7.21 FEMA mobile App FEMA.gov. (<http://www.fema.gov/mobile-app>.)

and alerts communicated across many strata. Mobile apps are an economical and highly efficient method of communication (Figure 7.21).

Mitigation teams play a crucial role in this stage of the natural or catastrophic event. At post-assessment, the team can determine the efficacy of risk reduction methods and simultaneously recommend protocols for improvement. Post-assessment is central to homeland policy making since it looks to

- Assess factors that contributed to disaster effects
- Identify risk reduction opportunities
- Educate the public and local government officials in methods to reduce future risks
- Promote hazard mitigation community planning and project development that will result in sustainable community development
- Provide grants to fund hazard mitigation projects
- Assist communities in marketing the NFIP
- Provide technical assistance to state, tribal, and local governments to utilize rebuilding as an opportunity for enhanced local codes and ordinances

7.3 FEMA Response and Recovery

How a nation responds to terror and disaster says much about its makeup and capacity to protect its citizens. The term *response* connotes many things, including immediate actions to save lives, protect property and the environment, and meet basic human needs.⁴³ Response also includes the execution of emergency plans and actions to support short-term recovery. The level of response will depend on the circumstances and conditions at specific locations.⁴⁴

The turmoil and anguish caused by the event are burdensome enough. When government fails to respond or does so in an unprofessional way, it simply adds to the pain and suffering of the general public. Nothing could have seared the national psyche more than the glaring



Figure 7.22 Thousands of people sought refuge in the New Orleans Convention Center, which was lacking in basic necessities and security as nightmarish stories of crime were told and retold.

ineptitude of state, local, and federal officials in the matter of Katrina.⁴⁵ The level of incompetence roused up even the most jaded of bureaucrats, and the toll from Katrina mounted and rose like the waters swirling about the New Orleans region.⁴⁶

When one looks back on these events, it is almost incomprehensible that government could function so miserably. In this sense, response and recovery are just as critical to the homeland professional as planning and preparation. In many ways, response and recovery need to be embedded in any concept of planning and preparedness. These actions are not divisible but united in purpose and practice. If there is any lesson from Katrina, it is that these two worlds cannot remain disjointed but must be intimately interconnected (Figure 7.22).

It is not enough to say that Katrina was a gargantuan storm—for that was self-evident. What is equally telling is the collapse of basic services while in a disaster. Things as simple as transportation assets, such as buses, which could have been utilized to ferry people away, were left to wallow in the water by the hundreds. Mayor Ray Nagin has been rightfully faulted for his malfeasance in this matter (Figure 7.23).⁴⁷

There are other instances of flat-out negligence in the handling of disasters, and there is a host of critics concerning the government's handling of the pandemic of 2020. In some cases, this is simply second-guessing and Monday-Morning quarterbacking. In many cases, it seems that politics often clouds learned assessment and evaluation in these difficult events.⁴⁸

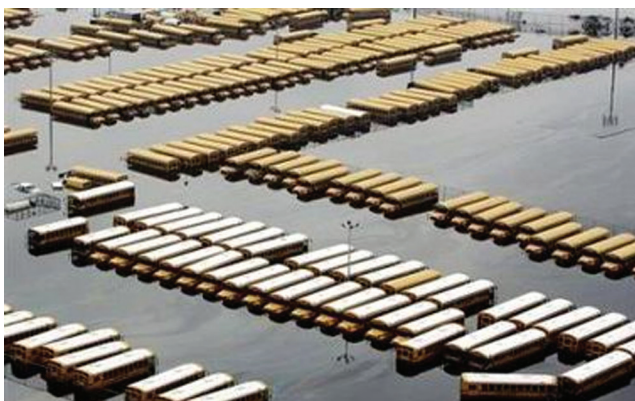


Figure 7.23 Buses in New Orleans during Hurricane Katrina.



Figure 7.24 Refrigerated trucks to store the dead in NYC: 3/31/2020. (Courtesy www.shutterstock.com.)

During the escalating days of the COVID-19 pandemic in New York City, the death and hospitalizations rates skyrocketed—so intensely that the hospital infrastructure, and even more poignantly, the staff of medical personnel entrusted with care and prevention of a pandemic getting out of control, were teetering on the edge of survival. Many felt the system was soon to be overwhelmed. Deaths were so rapidly occurring, that storage and processing of the dead become a major challenge (Figure 7.24).⁴⁹

In Hurricane Katrina, it was painfully obvious that a response and recovery protocol had completely escaped those entrusted with the disaster. As for the pandemic, the jury is still out, though many have lauded the Biden administration's quick response and mobilization to obtain and disseminate tens of millions of vaccines that have since been administered.

As a result, and in order to give a more stable and regularized set of protocols, DHS and FEMA authored an essential component of the homeland security model—the National Response Framework.⁵⁰

7.3.1 National Response Framework

The framework is a guide for a national, all-hazards response—from the smallest incident to the largest catastrophe.⁵¹ The framework identifies the key response principles, as well as the roles and structures that organize national response. How communities, states, the federal government, the private sector, and nongovernmental partners apply these principles for a coordinated, effective national response is the chief aim of the National Response Framework.⁵²

Internet Exercise: Familiarize yourself with the many resources relevant to a response plan by visiting the National Response Framework resource center at <https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response>.

The framework systematically incorporates public sector agencies at all levels, the private sector, and nongovernmental organizations. The framework also emphasizes the importance of personal preparedness by individuals and households. FEMA lays out the key principles of a functional and effective response plan in Figure 7.25.

The framework operates from very distinct and enlightened premises. Its ideology is primarily one of decentralization. Both FEMA and DHS appear to agree that the best understanding of any problem resides in those experiencing it. Local, decentralized response is usually more responsive than waiting in line for the federalists to show up. Here again, we saw clearly how New Orleans acted without decisiveness since it had been, at least in some ways, trained to await the federal invasion before acting itself. On top of this, the federal bureaucracy of FEMA and

Engaged Partnership with the Whole Community

Engaging the whole community is critical to successfully achieving a secure and resilient Nation, and individual and community preparedness is a key component. An effective partnership relies on engaging all elements of the whole community and, when appropriate, international partners. Engaged partnership and coalition building includes clear, consistent, effective, and culturally appropriate communication and shared situational awareness. Participation within these partnerships should include advocates for all elements of the whole community. The most effective partnerships within a community capitalize on all available resources—identifying, developing, fostering, and strengthening new and existing coordinating structures to create a unity of effort.

Scalability, Flexibility, and Adaptability in Implementation

Core capabilities should be scalable, flexible, and adaptable and executed as needed to address the full range of threats and hazards as they evolve. Scalable, flexible, and adaptable coordinating structures are essential in aligning the key roles and responsibilities to deliver the core capabilities. The flexibility of such structures helps ensure that communities across the country can organize efforts to address a variety of risks based on their unique needs, capabilities, demographics, governing structures, and non-traditional partners.

Integration Among the Frameworks

The five mission areas aid in organizing national preparedness activities. Core capabilities are highly interdependent and applicable to any threat or hazard. All five mission areas integrate with each other through interdependencies, shared assets, and overlapping objectives.

Three core capabilities span all five mission areas: Planning; Public Information and Warning; and Operational Coordination. The common core capabilities serve to unify the mission areas, promote unity of effort, and are essential foundations for the success of the remaining core capabilities.

In addition to the three common core capabilities, a number of other core capabilities involve more than one mission area (e.g., Protection and Prevention share a number of common elements and rely on many of the same core capabilities). Integration among mission area resources and processes is important to maximize core capabilities and minimize risk. Many of the core capabilities can be linked across mission areas through shared assets and services. For example, functionality provided through geospatial services that build situational awareness can be applied across multiple Response core capabilities, as well as core capabilities in the other four mission areas.

Figure 7.25 Response doctrine key themes.

aligned agencies are part of a lumbering giant that has no conception of its own limitations. Government is by nature a self-perpetuating, self-propagating entity that mutates into forms never imagined. When this occurs, the responsiveness that the ordinary citizen rightfully hopes for simply evaporates into a sea of paperwork and indecision. Hence, the response must first and foremost be a local one. As even FEMA points out:

Incidents begin and end locally, and most are wholly managed at the local level. Many incidents require unified response from local agencies, NGOs, and the private sector, and some require additional support from neighboring jurisdictions or the State. A small number require Federal support.⁵³

In a comparative sense, the Twin Towers experience edified the power and preeminence of local control. Few would argue that the City of New York, its police and fire departments, as well as its agencies from port authorities and neighboring states, did a superlative job during this challenging period (Figure 7.26).

New York City Mayor Rudy Giuliani led the city in its response, while in New Orleans, during Katrina, leadership was utterly missing. New Orleans Mayor Ray Nagin, now an indicted and convicted felon, and Governor Kathleen Blanco, then governor of Louisiana, became targets of constant derision in their handling of Katrina. Aside from not being prepared, the inadequacy of the response in these extreme circumstances was self-evident at every level of emergency response.



Figure 7.26 New York City police department at Ground Zero. (Courtesy of the NYPD Police Benevolent Association.)

In a nutshell, the comparison illustrates the dynamism known as response. As a result, a National Response Framework advances a partner-based model—fully recognizing that the locality can and will do a better job in response. Incidents must be managed at the lowest possible jurisdictional level and supported by additional capabilities at a higher level, if and when needed.

On the other hand, it is crucial that a chain of command and leadership be part of any response and recovery program. While DHS and FEMA both exhort local and state authorities to be major players in every form of threat and disaster, the scope and magnitude of these events sometimes make the federal authorities the dominant force, especially when requesting federal disaster aid and funds.

Internet Exercise: Read President Biden’s Emergency Declaration in Texas in response to the winter storm and massive power outages in February of 2021:

<https://www.fema.gov/press-release/20210214/president-joseph-biden-approves-emergency-declaration-texas>

Congress has tried to lay out standard protocols in the matter of jurisdiction and leadership, although resources often dictate the actions of the decision maker. Even so, federal agencies can and do shine when the lower level of government, the street level where the tragedy intimately unfolds, are equal partners rather than mere bystanders awaiting instructions.

Another feature of the National Response Framework is its inherent flexibility. Instead of a one-size-fits-all mentality, the framework urges emergency professionals to apply a response that fits the event. Incidents come in many shapes and sizes, and their complexity or simplicity will affect the nature of the response. As the framework recommends,

As incidents change in size, scope, and complexity, the response must adapt to meet requirements. The number, type, and sources of resources must be able to expand rapidly to meet needs associated with a given incident. The Framework’s disciplined and coordinated process can provide for a rapid surge of resources from all levels of government, appropriately scaled to need. Execution must be flexible and adapted to fit each individual incident. For the duration of a response, and as needs grow and change, responders must remain nimble and adaptable. Equally, the overall response should be flexible as it transitions from the response effort to recovery.⁵⁴

The response framework recommends a unified command structure in the mold and type as advanced in NIMS. Calling on responders to image the Incident Command System (ICS), the framework steadily encourages competing agencies to work in a unified way—without battles over territory or responsibility. The framework rightfully advances unity in command as

indispensable to response activities and requires a clear understanding of the roles and responsibilities of each participating organization. Success requires unity of effort, which respects the chain of command of each participating organization while harnessing seamless coordination across jurisdictions in support of common objectives. Use of the Incident Command System (ICS) is an important element across multi-jurisdictional or multiagency incident management activities. It provides a structure to enable agencies with different legal, jurisdictional, and functional responsibilities to coordinate, plan, and interact effectively on scene. As a team effort, unified command allows all agencies with jurisdictional authority and/or functional responsibility for the incident to provide joint support through mutually developed incident objectives and strategies established at the command level. Each participating agency maintains its own authority, responsibility, and accountability.⁵⁵

Finally, the framework advances the perpetual concept of readiness in the design of any response plan. Agencies must be prepared and ready to carry out the response mission. Agencies must understand the dilemma, have mastered the problem, and present themselves as being capable of a prepared and ready response.⁵⁶ Agencies must not victimize those harmed by delay in their operations or responsibilities. Agencies must move quickly in response and avoid the cumbersome delays that always emerge from a lack of preparation and readiness.⁵⁷ Not only must emergency and justice professionals know the risk that is to be dealt with, but just as compellingly, they need to place a high priority on the timeliness of response:

Acting swiftly and effectively requires clear, focused communication and the processes to support it. Without effective communication, a bias toward action will be ineffectual at best, likely perilous. An effective national response relies on disciplined processes, procedures, and systems to communicate timely, accurate, and accessible information on the incident's cause, size, and current situation to the public, responders, and others. Well-developed public information, education strategies, and communication plans help to ensure that lifesaving measures, evacuation routes, threat and alert systems, and other public safety information are coordinated and communicated to numerous diverse audiences in a consistent, accessible, and timely manner.⁵⁸

Internet Exercise: Visit the Nation Incident Management System website at <https://www.fema.gov/national-incident-management-system>.

Depending on the subject matter, the critical infrastructure in question, and the event itself, any response will need to be tailored to it. For example, the National Response Framework resource location provides response protocols for industries and businesses, critical infrastructure, and other likely targets in need of response. An excellent illustration of this response plan can be seen in transportation. Figure 7.27 is a sample page from the response plan.

For a complete look at a response plan for a biological attack, review the annex published by the National Response Framework in Appendix B.

7.4 Conclusion

The chapter delivers essential information on the role of FEMA. FEMA, once independent of DHS, was the country's agency of natural disaster. Floods, hurricanes, fires, and earthquakes consumed its planning and response mentality. Slowly but surely, and with extraordinary reservation, the FEMA model came to accept that the regimens and protocols for natural as well as man-made disasters in the form of terrorism are really the same. While this may be conceptually true, the fit of FEMA into DHS has been tougher than anticipated. Every imaginable type of threat and hazard receives some scrutiny in this chapter, though the emphasis is on planning and preparation—rather than on response and recovery.

This chapter covers the historic role of FEMA as well as its contemporary structure and organizational design under DHS. The chapter also heavily scrutinizes the role and purpose of the National Response Framework. In addition, the chapter emphasizes the role of preparedness in the FEMA mission, the importance of mitigation in the control and containment of disasters, and techniques of response and recovery.

Emergency Support Function #1 –Transportation Annex	
ESF Coordinator:	Support Agencies:
Department of Transportation	Department of Agriculture
	Department of Commerce
Primary Agency:	Department of Defense
Department of Transportation	Department of Energy
	Department of Homeland Security
	Department of the Interior
	Department of Justice
	Department of State
	General Services Administration
	U.S. Postal Service
INTRODUCTION	
Purpose	
Emergency Support Function (ESF) #1 - Transportation provides support to the Department of Homeland Security (DHS) by assisting Federal, State, tribal, and local governmental entities, voluntary organizations, nongovernmental organizations, and the private sector in the management of transportation systems and infrastructure during domestic threats or in response to incidents. ESF # 1 also participates in prevention, preparedness, response, recovery, and mitigation activities. ESF #1 carries out the Department of Transportation (DOT)'s statutory responsibilities, including regulation of transportation, management of the Nation's airspace, and ensuring the safety and security of the national transportation system.	
Scope	
ESF #1 embodies considerable intermodal expertise and public and private sector transportation stakeholder relationships. DOT, with the assistance of the ESF #1 support agencies, provides transportation assistance in domestic incident management, including the following activities: • Monitor and report status of and damage to the transportation system and infrastructure as a result of the incident. • Identify temporary alternative transportation solutions that can be implemented by others when systems or infrastructure are damaged, unavailable, or overwhelmed. • Perform activities conducted under the direct authority of DOT elements as these relate to aviation, maritime, surface, railroad, and pipeline transportation. • Coordinate the restoration and recovery of the transportation systems and infrastructure. • Coordinate and support prevention, preparedness, response, recovery, and mitigation activities among transportation stakeholders within the authorities and resource limitations of ESF #1 agencies.	

Figure 7.27 Response plan sample page.

Keywords

All-Hazards Response; Army Corps of Engineers; Catastrophic Event; Decentralization; Disaster; Exemplary Practice; Federal Broadcast System; Federal Disaster Assistance Administration; Flood Hazard Mapping; FloodSmart; Geographic Information System; Hazus-MH; Hurricane Liaison Team; Integrated Emergency-Management System; MAP MOD; Mitigation; Mitigation Assessment Team; Mitigation Planning; National Dam Safety Program; National Earthquake

Hazards Reduction Plan; National Fire Prevention Control Office; National Flood Insurance Program; National Hurricane Program; National Preparedness Directorate; Post Assessment Report; Preparedness; Project Impact; Protocol; Reconstruction Finance Corporation; Response and Recovery; Routine Emergency

Discussion Questions

1. Discuss the mission of FEMA prior to 9/11. Since 9/11, how has that mission been modified?
2. Why have there been growing pains for the new FEMA since incorporation into DHS?
3. Why is planning so critical to effective homeland policy?
4. Why does mitigation have a pre- and post-role in homeland defense?
5. Discuss areas where hazards are likely events in your community.
6. What type of mitigation plan would work well once a hazard has been identified?
7. Why do response and recovery involve important public relations issues?
8. What is the general thrust of agency cooperation between federal, state, and local entities?
9. In what region of FEMA does your jurisdiction lie?
10. If a hazard or disaster took place in your region, what agency would likely be the lead player in response and recovery?
11. Compare the preparedness and response exhibited in Hurricane Katrina versus Hurricane Sandy.

Practical Exercises

1. Enroll and take the training of FEMA regarding the reading and interpretation of flood maps at <http://www.fema.gov/online-tutorials>.
2. Visit FEMA's software tool for mitigation at <https://www.fema.gov/flood-mapping-products>.
3. Discover best practices of interest to your community. Visit the FEMA database of best practices at <http://www.fema.gov/mitigation-best-practices-portfolio>.
4. Take a tour of the National Response Framework at <http://www.fema.gov/national-response-framework>.

Notes

- 1 J. A. Bullock et al., *Introduction to Homeland Security* (New York: Elsevier, 2005), 6.
- 2 R. T. Stafford, *Disaster Relief and Emergency Assistance Act*, P.L. 100-707, signed into law November 23, 1988; amended the *Disaster Relief Act of 1974*, P.L. 93-288. This act constitutes the statutory authority for most federal disaster response activities, especially as they pertain to FEMA and FEMA programs.

Homeland Security

- 3 FEMA, About the agency, <http://www.fema.gov/about> (accessed August 18, 2020).
- 4 FEMA, Organization chart, <https://www.fema.gov/about/organization> (accessed August 18, 2020).
- 5 See: FEMA National Advisory Council, Modernizing the Nation's Public Alert and Warning System (February 15, 2019), https://www.fema.gov/media-library-data/1572035345771-de48b48b67b533f-604c9b23e9625aa01/NAC_IPAWS_Subcommittee_Final_Report.pdf (accessed August 18, 2020).
- 6 FEMA National Advisory Council, Report to the FEMA Administrator, (November 2019), https://www.fema.gov/media-library-data/1576076713587-c1ae1017f2adb4b836ad3db0c26d3578/November_2019_NAC_Report_final.pdf (accessed August 18, 2020).
- 7 FEMA, Regions webpage, <https://www.fema.gov/fema-regional-contacts> (accessed August 18, 2020).
- 8 FEMA, 2018–2022 Strategic Plan, 4 (2018), https://www.fema.gov/media-library-data/1533052524696-b5137201a4614ade5e0129ef01cbf661/strat_plan.pdf (accessed August 18, 2020).
- 9 Center for Disaster Philanthropy, The role of FEMA in disasters, <https://disasterphilanthropy.org/issue-insight/fema/> (accessed August 18, 2020).
- 10 W. F. Shughart II, Disaster relief as bad public policy, *The Independent Review*, 15(4) (Spring 2011): 530.
- 11 R. Wimberly, First-Ever National EAS Test Will Come from the White House, *Emergency Management*, <http://securitydebrief.com/2011/03/23/first-ever-national-eas-test-will-come-from-the-white-house/>, March 21, 2011 (accessed August 18, 2020).
- 12 FEMA, The Integrated Public Alert and Warning System (IPAWS) Presentation, 9 (2017), https://www.fema.gov/media-library-data/1497530734477-cd049c3b6c0e3d8d224080a7a9ac3839/IPAWS_101_Presentation_04212017.pdf (accessed August 18, 2020).
- 13 See: FEMA, Integrated Public Alert & Warning System, <https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system> (accessed August 18, 2020).
- 14 For an example, see: FEMA, Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide, 3rd Edition (May 2018), https://www.fema.gov/media-library-data/1527613746699-fa31d9ade55988da1293192f1b18f4e3/CPG201Final20180525_508c.pdf (accessed August 18, 2020).
- 15 See FEMA website, <https://www.fema.gov> (accessed August 18, 2020).
- 16 See: Disaster Assistance. Gov, News Feeds webpage, <https://www.disasterassistance.gov/information/news-feeds> (accessed August 18, 2020).
- 17 Department of Homeland Security, FEMA: Radiological Emergency Preparedness Program Manual and Supplement, 2011.
- 18 For an overview of Preparedness for the Citizen and the Community, see http://www.fema.gov/pdf/areyouready/basic_preparedness.pdfm (accessed August 18, 2020). See also FEMA's website for many guides and plans; go to www.fema.gov/media-library and search "family communication plan." See also: <https://www.fema.gov/individual-and-community-preparedness-division>
- 19 For a general series of considerations on planning and preparation, see R. W. Perry and M. K. Lindell, Preparedness for emergency response: Guideline for the emergency planning process, *Disasters*, 27 (2003): 336–350.
- 20 Department of Homeland Security, Safe Rooms and Shelters—Protecting People against Terrorist Attacks National Geospatial Preparedness Needs Assessment, May 2006, Figure 4.3.
- 21 Department of Homeland Security, Safe Rooms and Shelters, Figure 4.1.
- 22 Department of Homeland Security, Using HAZUS-MH for Risk Assessment: How-to Guide, August 2004. See also: US Department of Homeland Security, Hazus-MH User Manual, https://www.fema.gov/media-library-data/20130726-1820-25045-8814/hzmh2_1_fl_um.MA (accessed August 18, 2020).
- 23 For a look at disaster preparedness, see National Fire Protection Association, Implementing NFPA 1600: National Preparedness Standards, D. Schmidt, editor (Quincy, MA: National Fire Protection Association, 2008).
- 24 FEMA, Hazus software, <https://www.fema.gov/hazus-software> (accessed August 18, 2020).
- 25 K. Vlahos, A season of wild wind, *Wind & Water*, *Homeland Security Today*, August, 2011: 34.
- 26 Ibid.
- 27 <https://www.fema.gov/security-risk-management-series-publications>
- 28 FEMA, Risk Management Series, <https://www.fema.gov/security-risk-management-series-publications> (accessed August 30, 2009).

- 29 Congressional Research Service, *FEMA's Pre-Disaster Mitigation Program: Overview and Issues* 21 (Washington, DC: Congressional Research Service, 2009).
- 30 O. O. Olonilua and O. Ibitayo, *Toward multihazard mitigation: An evaluation of FEMA-approved hazard mitigation plans under the Disaster Mitigation Act of 2000*, *Journal of Emergency Management*, 9 (January/February 2011): 37–49, 48.
- 31 FEMA, *Guide for all-hazard emergency operations planning*, Chapter 4, 1996, www.fema.gov/pdf/plan/4-ch.pdf (accessed August 18, 2020).
- 32 Congressional Research Service, *National Flood Insurance Program: Background, Challenges, and Financial Status* (Washington, DC: Congressional Research Service, 2011).
- 33 FEMA, *National Flood Insurance Program Terminology Index*, <https://www.fema.gov/significant-flood-events> (accessed August 18, 2020).
- 34 FEMA P-55, *Coastal Construction Manual: Principles and Practices of Planning, Siting, Designing, Constructing, and Maintaining Residential Buildings in Coastal Areas*, 4th Edition (2011).
- 35 See: FEMA, *Mitigation Assessment Team Report: Hurricane Michael in Florida*, (February 2020), https://www.fema.gov/media-library-data/1582559571919-8b4ba5ce4c75d0b4f73c7f69215451f1/901907_FEMA_MAT_Michael_508_02-21-2020_FINAL.pdf (accessed August 18, 2020); See also: Ready Business, *Hurricane Toolkit*, https://www.ready.gov/sites/default/files/2020-04/ready_business_hurricane-toolkit.pdf (accessed August 18, 2020).
- 36 See: US Dept of Homeland Security, *Ready Business*, <https://www.ready.gov/business> (accessed August 18, 2020).
- 37 Ready Business, *Hurricane Toolkit*, https://www.ready.gov/sites/default/files/2020-04/ready_business_hurricane-toolkit.pdf (accessed August 18, 2020).
- 38 For an excellent resource on flood and wind damage, see FEMA *Floods and Maps Products and Tools* page, <https://www.fema.gov/flood-maps/products-tools> (accessed August 18, 2020).
- 39 FEMA, *FloodSmart Online Tools and Resources Flyer*, https://www.fema.gov/media-library-data/20130726-1912-25045-6398/fs_toolsandresourcesforstakeholders_032013.pdf (accessed August 18, 2020).
- 40 FEMA, *FloodSmart.Gov*, <https://www.floodsmart.gov/community> (accessed August 18, 2020); FEMA, *FloodSmart Online Tools and Resources Flyer*, https://www.fema.gov/media-library-data/20130726-1912-25045-6398/fs_toolsandresourcesforstakeholders_032013.pdf (accessed August 18, 2020).
- 41 Federal Emergency Management Agency, *PARTNERSHIPS IN PREPAREDNESS: A Compendium of Exemplary Practices in Emergency Management*, Volume II, May 1997, http://www.fema.gov/media-library-data/20130726-1447-20490-3555/exp_v2_1_1.txt (accessed August 18, 2020).
- 42 Congressional Research Service, *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations* (Washington, DC: Congressional Research Service, 2011).
- 43 R. McCreight, *Establishing a national emergency response and disaster assistance corps*, *Homeland Defense Journal*, 10 (September 2007); C. Hines, *Disaster management*, *Law & Order*, 58 (August 2006): 54.
- 44 For an example of how distinctly and very differently FEMA would act in the case of a Dirty Bomb, see Congressional Research Service, *"Dirty Bombs": Technical Background, Attack Prevention and Response*, Issues for Congress, 2011, <http://www.fas.org/sgp/crs/nuke/R41890.pdf> (accessed August 18, 2020).
- 45 See J. Flynn, *Review of disasters and the law: Katrina and beyond*, *Journal of Homeland Security and Emergency Management*, 1 (2007): 4.
- 46 There is little question that FEMA was rightfully criticized. One benefit from the criticism was an avalanche of new research in the area, such as R. McCreight, *Aspects of emergency management*, *Homeland Defense Journal*, 5 (May 2007): 22–28; J. Dowle, *Prepare for homeland security*, *Law & Order*, 5 (May 2007): 55; H. Stone, *Emergencies and action plans*, *Security*, 62 (October 2006): 43; R. Elliott, *State of readiness*, *Security Management*, 50 (December 2006): 51–57; and C. Perrow, *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial and Terrorist Disasters* (Princeton, NJ: Princeton University Press, 2007).
- 47 If we did this poorly at Katrina, how would we handle a tsunami? See A. Kimery, *Next tsunami*, *Homeland Security Today*, July, 2011: 34.

Homeland Security

- 48 For example, see: Nathaniel Weixel and Brett Samuels, Trump faces criticism over lack of national plan on coronavirus, May 16, 2010, The Hill, <https://thehill.com/homenews/administration/498078-trump-faces-criticism-over-lack-of-national-plan-on-coronavirus> (accessed August 18, 2020).
- 49 See: A. Venugopal, Dispatch from a Coronavirus Morgue Truck Worker: “They Write a Check for Your First Day, In Case You Don’t Come Back,” April 16, 2020, <https://gothamist.com/news/dispatch-morgue-truck-worker-coronavirus-covid-nyc> (accessed August 18, 2020).
- 50 For a list of authorities that permit federal, state, and local authorities to engage in homeland defense and intervention, at <http://www.fema.gov/pdf/emergency/nrf/nrf-authorities.pdf> (accessed August 18, 2020).
- 51 See Department of Homeland Security, National Response Framework Fact Sheet, https://www.fema.gov/media-library-data/1544456661952-f2ee7ccbf5991097b1656202e5a491b8/Revised_NRF_Update_Information_Sheet.pdf (accessed August 18, 2020).
- 52 A. Bitto, Say what? Who? Me? Right here in the trenches? Collaborate or what? Seeking common ground in regional all-hazards preparedness training, *Journal of Environmental Health*, 69 (January/February 2007): 28–33.
- 53 Department of Homeland Security, National Response Framework, January 2008, 9. Despite this preference, national exercises are still in vogue at FEMA, though the 2020 program was cancelled due to the pandemic. DHS still sponsors National Level Exercise programs. See E. Pitman, National response, *Emergency Management*, March/April, 2011: 30; See also the 2019 National Level Exercise, <https://www.fema.gov/media-library-data/1551805608248-03bfe4a30169b06ad08a4bc443a8c180/Shakenf.pdf> (accessed August 18, 2020).
- 54 Department of Homeland Security, The National Response Framework (Washington, DC: U.S. Government Printing Office, January 2008), 10, <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf> (accessed August 18, 2020).
- 55 Department of Homeland Security, National Response Framework, 10.
- 56 Department of Homeland Security, National Response Framework, 27.
- 57 See R. Humphress, Building an emergency response competency system: Optimizing emergency personnel mobilization, *Journal of Homeland Security and Emergency Management*, 1 (2007): 4; D. Barbee, Disaster response and recovery: Strategies and tactics for resilience, *Journal of Homeland Security and Emergency Management*, 1 (2007): 4; D. Philpott, Emergency preparedness communications, *Homeland Defense Journal*, 44 (June 2007).
- 58 Department of Homeland Security, National Response Framework, 10–11.

8

Intelligence

OBJECTIVES

1. To comprehend the nature of the intelligence cycle
2. To outline the Department of Homeland Security's (DHS) intelligence-gathering approach in the aftermath of 9/11
3. To define the mission of the Federal Bureau of Investigation (FBI) as it relates to intelligence gathering and sharing
4. To list the various new policies, programs, and initiatives of the FBI since 9/11
5. To define the mission of the Central Intelligence Agency (CIA) as it relates to intelligence gathering and sharing
6. To list the various new policies, programs, and initiatives of the CIA and Department of Defense branches since 9/11
7. To list the mission, policies, programs, and initiatives of the new Office of the Director of National Intelligence (ODNI)
8. To list the mission, policies, programs, and initiatives of the Defense Intelligence Agency (DIA) since 9/11

8.1 Introduction

Much is expected of those entrusted with homeland protection. At a minimum, there is the expectation of basic security and safety—the notion that the homeland will be safe from attack from both domestic and foreign enemies. As already noted, exactly what the functionaries of homeland security should tackle is an evolutionary project. Today's threat may be tomorrow's less worrisome problem. However, there are certain core competencies that the professional class of employees in homeland security need to master. These are the nonnegotiable skill sets that the homeland system must demonstrate competence in. These are the essential underpinnings of what makes the homeland system work in any context. These competencies include:

- Intelligence
- Border security

Homeland Security

- Immigration
- Transportation security
- Public health

8.2 Intelligence

The task of intelligence gathering and analysis could be considered an overreaching competence, for just about everything in homeland security is guided by what we do, or should, or must know. Intelligence, in a sense, is the lifeblood of operations. Sometimes practitioners witness the mindlessness, the almost unintelligent rules, laws, and regulations, that policymakers impose. In other words, the bureaucratic mindset, in some cases, simply acts without intelligence because it acts or has been acting in a particular way for so long. Intelligence is more than mindless motion.¹ The idea of intelligence can be discerned in a host of contexts—domestic and international, military and covert, criminal and civil—as well as homeland security. Intelligence is, at its base, nothing more than information assessment. One way of describing it might be as follows:

The intelligence cycle is an iterative process in which collection requirements based on national security threats are developed, and intelligence is collected, analyzed, and disseminated to a broad range of consumers. Consumers sometimes provide feedback on the finished intelligence products, which can be used to refine any part of the intelligence cycle to ensure that consumers are getting the intelligence they need to make informed decisions and/or take appropriate actions.²

Intelligence activities largely reflect the agency mission and overall purpose of the task at hand. In some circles, intelligence is broken down into various disciplines. “Three major intelligence disciplines or ‘INTs’—signals intelligence (*sigint*), imagery intelligence (*imint*), and human intelligence (*humint*)—provide the most important information for analysts and absorb the bulk of the intelligence budget.”³ See Figure 8.1.⁴

Some might argue that homeland intelligence is a unique animal invented in the last 15 years. Others claim that intelligence is an interconnected dynamic—that homeland information can only come about in a holistic context, and that homeland security is impossible without the larger Intelligence Community inputting information. See Figure 8.2.

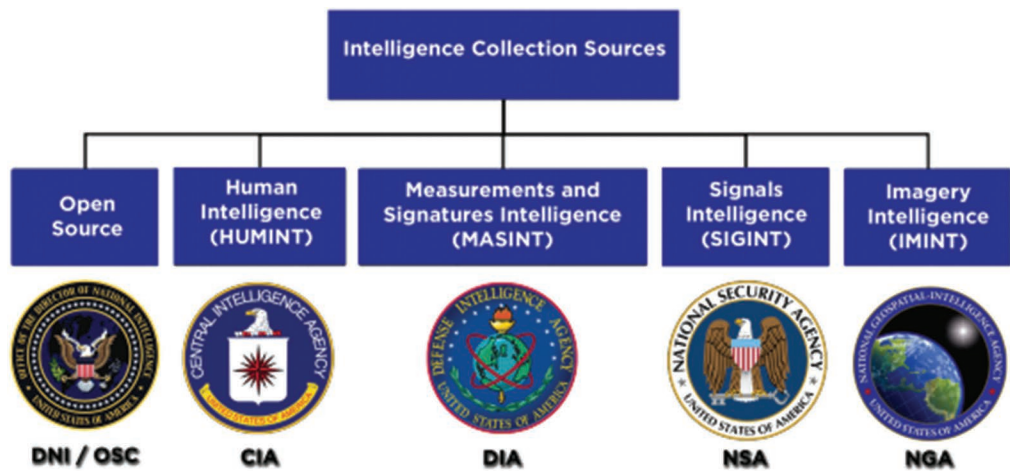


Figure 8.1 The various intelligence collection sources.



Figure 8.2 Logo for the U.S. Intelligence Community.



Figure 8.3 Intelligence-gathering matrix. (From CRS, *Homeland Security Intelligence* (Washington, DC: Library of Congress, 2006), 5.)

Homeland security is no better or worse than its aligned agencies of intelligence gathering. Figure 8.3 portrays this interdependence.⁵

DHS tends to favor this integrative approach and for good reason. If there was any persistent critique of government in the aftermath of 9/11, it was the failure of intelligence. But even more compellingly, the critics and commissions repeatedly castigated the Intelligence Community for its failure to share, to disseminate, and to work collaboratively with sister and brother agencies. Intelligence was boxed in prior to 9/11; it was departmentalized and compartmentalized rather than scrutinized in the national, integrative framework. Former secretary of DHS Michael Chertoff eloquently described this dilemma:

Intelligence, as you know, is not only about spies and satellites. Intelligence is about the thousands and thousands of routine, everyday observations and activities. Surveillance, interactions—each of which may be taken in isolation as not a particularly meaningful piece of information, but when fused together, gives us a sense of the patterns and the flow that really is at the core of what intelligence analysis is all about. ... We [DHS] actually generate a lot of intelligence ... we have many interactions every day, every hour at the border, on airplanes, and with the Coast Guard.⁶

Homeland Security

In this sense, intelligence is merely information shared that might give meaning. It is the patterns and connections that analysts are looking for. It is the overall fit of the information into particular facts and circumstances that the intelligence analyst seeks. And when intelligence works, it prevents the harm and terror from gaining a foothold. Recent killings by jihadis in San Bernardino seem to have escaped the Intelligence Community over a nearly 4-year cycle of indoctrination and terrorist formation. The same critique is applicable to the Saudi terrorist, training as a pilot at Pensacola, Florida airbase. See Figure 8.4.

How could a person harboring such beliefs, be trained amongst Navy pilots, as a favor to Saudi Arabia, yet our intelligence community missed all the signs?⁷ See Figure 8.5.⁸



Figure 8.4 Mohammed Alshamrani: the Saudi Officer killed three officers and injured eight others in an attack on Naval Air Station Pensacola, Florida on December 6, 2019.



Figure 8.5 Vice Adm. Mary Jackson, commander, Navy Installations Command, meets with Navy Security Force personnel at Naval Air Station Pensacola Dec. 12, 2019. The NSF personnel were first on scene during the Dec. 6, 2019 active shooter incident on base. (US Navy photo by Chief Mass Communication Specialist David Holmes.)

As a corollary, the United States targeted the head of the Islamic Revolutionary Guard Corp-Quds Force⁹, Qasem Soleimani in a hotly debated and controversial move by the Trump Administration. Soleimani was known to have been responsible for the design and planting of IED devices on various fields of battle as well as other tactics and clandestine operations some would argue directly supported and carried out terrorism. Still, his death was lauded by some and harshly criticized by others. See Figure 8.6.¹⁰

DHS and the intelligence community continue to make improvements in how information is shared. For example, the HSIN-Intel program is a notice center, a repository—almost a virtual bulletin board to keep all the governmental players updated on crucial Intelligence. See Figure 8.7.¹¹

Just as crucially, the idea of intelligence has become fixated on things beyond basic knowledge, and in a sense, tends toward technology and gadgets over the basic acquisition of information. Many professionals in the Intelligence Community remind us that intelligence is first and foremost knowledge—something gathered and then disseminated. Mark M. Lowenthal, president of the Security and Intelligence Academy, has long been a critic of our tendency to forget about the “basics” in intelligence gathering, and he urges us to “get back to the ‘knowledge building’ business.”¹²

From the outset of the agency, DHS looked squarely and keenly into the world of intelligence and saw the necessity for integration and cohesion among all governmental agencies. Indeed, in early 2002, so did Congress by enacting the Homeland Security Act, which not only contained the administrative underpinnings of DHS, but set the professional parameters of intelligence.¹³ The act precisely mandates and lays out expectations regarding the gathering of information and intelligence. It forces government as a whole to collaborate rather than insulate and contains provisions for information analysis and intelligence within DHS. The act does not transfer to DHS existing government intelligence and law enforcement agencies but envisions an analytical office utilizing the products of other agencies—both unevaluated information and finished



Figure 8.6 Qasem Soleimani, longtime head of Revolutionary Guard Corps-Quds Forces.



Homeland Security Information Network (HSIN)

www.dhs.gov/hsin-intelligence

Figure 8.7 The HSIN-Intel fact sheet.

reports—to provide warning of terrorist attacks, assessments of vulnerability, and recommendations for remedial actions at federal, state, and local levels, and by the private sector. In 2003, DHS set up the Terrorist Threat Integration Center (TTIC), an entity directed to assess threats, but then just as commandingly ordered the sharing and collaborative interchange of said intelligence (Figure 8.8).



Figure 8.8 TTIC logo.

The TTIC was established to:

- Optimize the use of terrorist threat–related information, expertise, and capabilities to conduct threat analysis and inform collection strategies
- Create a structure that ensures information sharing across agency lines
- Integrate terrorist-related information collected domestically and abroad in order to form the most comprehensive possible threat picture
- Be responsible and accountable for providing terrorist threat assessments for our national leadership

The TTIC was subsequently merged and renamed the National Counterterrorism Center, under the control and supervision of the U.S. director of national intelligence.¹⁴

8.3 Terror, Threats, Disaster, and Intelligence Agencies

The array of federal agencies dedicated to the task of intelligence is simply mind-boggling. Long before 9/11, the governmental and military complex was incessantly in need of intelligence. Governments cannot be run, wars fought, or borders secured without intelligence, nor can. Nor is intelligence gathering a system without restraint nor counterbalanced by competing legal traditions that honor privacy. The American experiment seeks to balance these demands.¹⁵

Intelligence has been part of our national fabric since the days of the American Revolution. In another portion of this chapter, we examine intelligence and defense of the homeland from the post–Civil War period, to the Cold War, to the riots of the 1960s, and end in the present. In each time frame, those who labor to protect the country need intelligence. After 9/11, these agencies had to adjust and redefine traditional definitions and outlooks on exactly what intelligence is effective. Added to the agency demands was the world of terror—an evolving terror erected by the jihadists and those who hate the American experience. It changed the way the intelligence business is carried out. To be sure, even DHS sees intelligence as a core function of its purpose and operational philosophy. DHS’s Office of Intelligence and Analysis has four strategic goals:

- Promote understanding of threats through intelligence analysis
- Collect information and intelligence pertinent to homeland security
- Share information necessary for action
- Manage intelligence for the homeland security enterprise

Homeland Security

Its structure reflects the multivariate nature of intelligence, with special sections dedicated to counterintelligence (CI) and counterterrorism as well as border and intelligence management (see Figure 8.9).¹⁶

Terror is not a new reality since 9/11 for federal and state justice agencies. While the attacks of 9/11 surely enhanced the nature of global terrorism in the domestic sphere, law enforcement leadership could not have been surprised by the possibility or actuality of any attack on American soil. The U.S. Intelligence Community generally comprises these agencies:

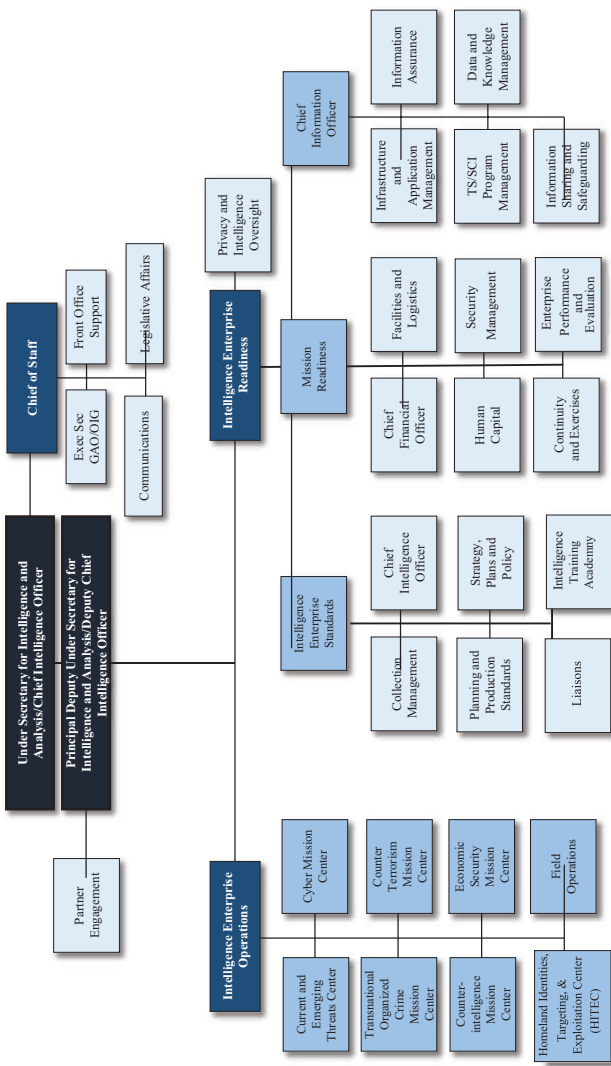
- Office of the Director of National Intelligence
- Office of the National Counterintelligence Executive
- Information-Sharing Environment
- National Counterterrorism Center
- National Intelligence Council
- Central Intelligence Agency
- Drug Enforcement Agency
- Defense Intelligence Agency
- Federal Bureau of Investigation
- Information Sharing Environment
- Marine Corps Intelligence
- National Cybersecurity and Communications Integration Center
- National Geospatial Intelligence Agency
- National Reconnaissance Office
- National Security Agency
- Office of Naval Intelligence
- U.S. Air Force Office of Special Investigations
- U.S. Army Intelligence and Security Command
- U.S. Coast Guard
- U.S. Department of Energy
- U.S. Department of Homeland Security
- U.S. Department of State
- U.S. Treasury Department

Throughout this book, the reader has been exposed to many members of the homeland security community. It is impossible to cover it all due to its sheer size and scope. What follows is a cursory look at the historic and emerging agencies entrusted with diverse intelligence responsibilities (Figure 8.10).¹⁷

8.3.1 Federal Bureau of Investigation

The FBI has held jurisdictional authority in matters involving terrorism since 1986. Indeed, the FBI had been busy with all sorts of terrorist activity since the early 1980s. In its long and distinguished history, the FBI has been called on in a wide array of law enforcement initiatives, from rackets and organized crime to public corruption, from attacks on U.S. embassies to terror plots against the United States.

I&A Organizational Alignment



August 2018

Figure 8.9 Office of Intelligence and Analysis organization chart.



Figure 8.10 DEA Intelligence Center, El Paso, Texas.

The FBI has long been an agency capable of adaptation and mission adjustment—a characteristic referred to as *change of mandate*. This is one of its greatest strengths—that it is capable of addressing new and emerging threats to the country (Figure 8.11).

One of its most glaring weaknesses has been its upper echelon leadership to, at times, become political pawns. The FBI needs to return to its first principles and remove itself from all things political. When it is on task, and its rank and file can carry out their mission, there is no better law enforcement agency. See Figure 8.12.¹⁸



Figure 8.11 FBI Hostage Team training in Quantico: fbi.gov.

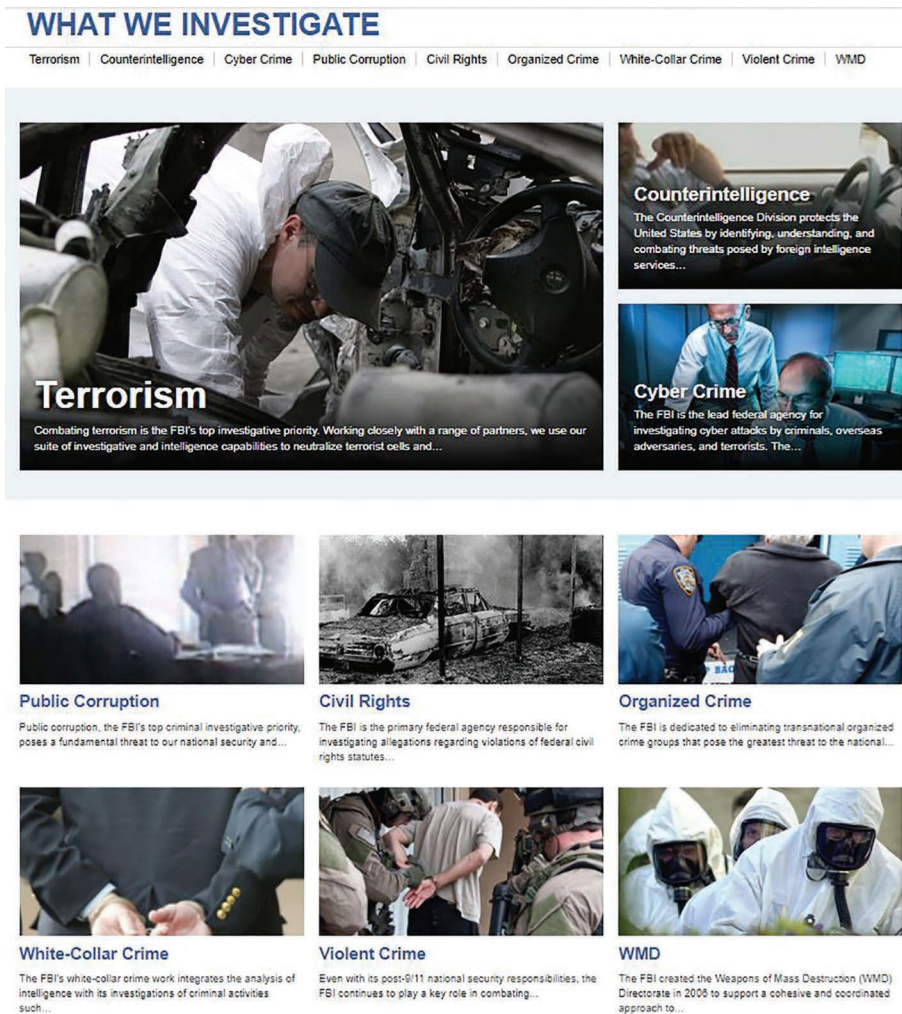


Figure 8.12 The many arenas in which the FBI conducts its investigations.

Internet Exercise: For the history of the FBI, see <https://www.fbi.gov/about-us/history/brief-history>.

The FBI has extensive experience in the world of intelligence and espionage, but these skills were largely shaped after World War II and the emergence of the Cold War. For nearly 40 years, the FBI's main thrust in the world of international activity coalesced around Cold War enemies rather than modern-day jihadists wishing the end of America and its allies. While the skill set may be complementary in both worlds, there is little question that the FBI realized that its world and the world around was changing. In the late 1980s and throughout the 1990s, the soil of the United States was stained with domestic terrorism. Both the Oklahoma City bombing, and the World Trade Center attacks triggered a new approach at the FBI. The shift largely dwelled on the impact of terrorism, both domestically and internationally. After 9/11, the FBI was increasingly asked to adjust and adapt its mission to contend with terror threats.

At this time, Director Christopher Wray has been a quiet leader trying to take corrective action, but his critics, including Judicial Watch and many in Congress, are perplexed by his slow-walking methods. On his watch the FBI is either going to depoliticize or continue to generate

Homeland Security

mistrust. Insofar as emerging threats, Wray provided testimony in Senate hearings on March 2, 2021 regarding extremism that led to the January 6, 2021 storming of the United States Capitol and insurrection. In his testimony he condemned the attack on the U.S. Capitol as domestic terrorism.¹⁹ Wray continued on as Director, and was retained, by the Biden administration. See Figure 8.13.²⁰

From 2001 onward, the FBI has continuously designed new programs and initiatives as well as fine-tuned existing programs to reflect the never-ending challenges of terror, but it must shake the scandals that envelop it to be more effective. Of particular interest has been the rise of joint operations with African nations where jihadis and terrorists are planting new operational seeds. For example, the FBI has now partnered with certain countries, like Kenya in establishing terror deterrence mechanisms such as the JTTF—to be covered in the next section.²¹ See Figure 8.14.²²



Figure 8.13 Christopher A. Wray.



Figure 8.14 The FBI frequently, and increasingly, partners with countries—such as the Kenyan representatives shown here—to establish terrorism deterrence capabilities.

8.3.1.1 Joint Terrorism Task Forces

The FBI reinforced the importance and operational role of the joint terrorism task forces (JTTFs), an amalgam of state, federal, and local law enforcement in major American cities such as New York. There are more than 200 JTTFs presently operating, 56 of which are housed in local FBI headquarters. At the federal level, full-time membership in the JTTF is granted automatically to the following entities:

- FBI
- U.S. Marshals Service
- Bureau of Alcohol, Tobacco, and Firearms
- U.S. Secret Service
- U.S. State Department/Diplomatic Security Service
- Immigration and Customs Enforcement
- U.S. Border Patrol
- Postal Inspection Service
- Treasury Inspector General for Tax Administration
- Internal Revenue Service
- U.S. Park Police
- Federal Protective Service
- Department of Interior's Bureau of Land Management
- Defense Criminal Investigative Service
- Air Force Office of Special Investigations
- U.S. Army
- Naval Criminal Investigative Service
- Central Intelligence Agency
- State and Local Law Enforcement

See Figure 8.15.²³

In nearly 60 major American centers, JTTFs were operating before the Twin Towers or the Pentagon were ever struck. After the attack, increased emphasis on the role of intelligence was evident in the sheer increase of JTTF entities, with 104 distinct organizations established since 9/11.²⁴ For a representative example of a JTTF, review the organization and structure of Albany, New York. The Albany JTTF combines federal, state, and local police forces, the U.S. Postal Service, as well as geographically aligned agencies that work in close proximity to the task force (see Figure 8.16).

Of recent interest has been the nationwide collaboration and cooperation between JTTFs and fusion centers. No two entities could better prove the advantages of information sharing than these entities. While JTTFs get their information from a variety of sources, fusion centers also aid in the sharing of intelligence and assist by providing information gathered through combining the knowledge, expertise, and information resident within law enforcement and homeland security agencies operating throughout the nation.²⁵ In the recent attempt of a car bomber in Times Square, New York, the cooperation of the JTTF and the fusion center model were obvious to those investigating the case (Figure 8.17).



Figure 8.15 Two FBI members of the JTTF.

Albany, NY Joint Terrorism Task Force (JTTF)

The JTTF is responsible for all domestic and international terrorism matters in the two-state territory. The JTTF mission is to prevent acts of terrorism before they occur, and to effectively and swiftly respond to any actual criminal terrorist act by identifying and prosecuting those responsible. The following agencies participate in the JTTF on a full-time or part-time basis:

- * Central Intelligence Agency
- * US Bureau of Alcohol, Tobacco and Firearms
- * US Immigration and Customs Enforcement
- * US Internal Revenue Service
- * US Department of State (Bureau of Diplomatic Security)
- * US Marshals Service
- * US Postal Inspection Service
- * New York State Office of Inspector General
- * New York State Police and Vermont State Police
- * Albany, New York, Police Department
- * Schenectady, New York, Police Department
- * Troy, New York, Police Department

Figure 8.16 About the Albany, New York, Joint Terrorism Task Force. (<https://www.fbi.gov/history/field-office-histories/albany>.)

8.3 Terror, Threats, Disaster, and Intelligence Agencies



Figure 8.17 Faisal Shazhad: Homegrown terrorist attempt in Times Square.

8.3.1.2 National Security Branch

The National Security Branch (NSB), established on September 12, 2005, combines the missions, capabilities, and resources of the counterterrorism (CT), CI, and intelligence elements of the FBI under the leadership of a senior FBI official. The NSB reflects the new focus of the FBI by assigning a significant portion of its manpower and resources to the detection, elimination, and prevention of terrorist activity (Figure 8.18).²⁶



Figure 8.18 FBI National Security Branch logo.

OUR VISION

Ahead of the threat through leadership, agility, and integration.

OUR MISSION

To protect the American people and uphold the Constitution of the United States.

OUR PRIORITIES

- Protect the United States from terrorist attack
- Protect the United States against foreign intelligence operations and espionage
- Protect the United States against cyber-based attacks and high-technology crimes
- Combat public corruption at all levels
- Protect civil rights
- Combat transnational/national criminal organizations and enterprises
- Combat major white-collar crime
- Combat significant violent crime

<https://www.fbi.gov/about/mission>

The aim and purpose of the NSB is summarized by its mission and vision. The NSB focuses on four major initiatives within the bureau: counterterrorism, counterintelligence, terrorist screening, high value detainee interrogation, and weapons of mass destruction (WMDs). An organizational chart is shown in Figure 8.19.²⁷

The counterterrorism unit tracks known and suspected terrorists in its Terrorist Screening Center (TSC). The TSC now provides “one-stop shopping” so that every government screener is using the same terrorist watch list—whether it is an airport screener, an embassy official issuing visas overseas, or a state or local law enforcement officer on the street.²⁸ The TSC allows government agencies to run name checks against the same comprehensive list with the most accurate, up-to-date information about known and suspected terrorists (Figure 8.20).

In the area of intelligence gathering, the FBI extends its efforts across the world by using diverse approaches in the gathering of pertinent information. The general approaches are as follows:

- Human intelligence (HUMINT) is the collection of information from human sources. The collection may be done openly, as when FBI agents interview witnesses or suspects, or it may be done through clandestine or covert means (espionage).
- Signals intelligence (SIGINT) refers to electronic transmissions that can be collected by ships, planes, ground sites, or satellites.
- Imagery intelligence (IMINT) is sometimes also referred to as photo intelligence (PHOTINT).
- Measurement and signatures intelligence (MASINT) is a relatively little-known collection discipline that concerns weapons capabilities and industrial activities. MASINT includes the advanced processing and use of data gathered from overhead and airborne IMINT and SIGINT collection systems.
- The DIA’s Central MASINT Office (CMO) is the principal user of MASINT data. Measurement and signatures intelligence has become increasingly important due to growing concern about the existence and spread of WMDs.
- Open-source intelligence (OSINT) refers to a broad array of information and sources that are generally available, including information obtained from the media.

8.3.1.3 NSB and the WMD Directorate

In July 2006, the WMD Directorate was created within the NSB to integrate WMD components previously spread throughout the FBI (Figure 8.21).

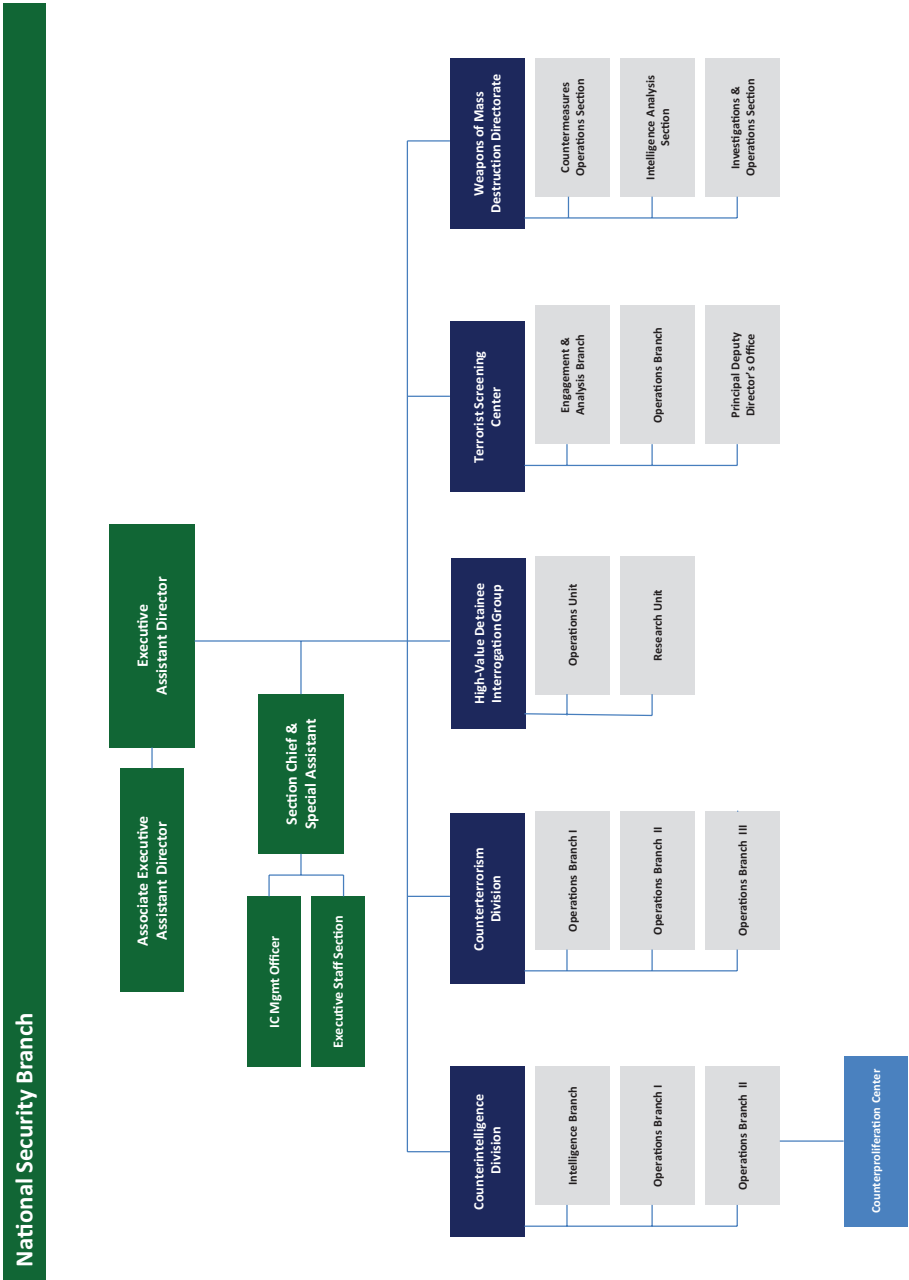


Figure 8.19 FBI National Security Branch organizational chart.



Figure 8.20 Seal of the Terrorist Screening Center.



Figure 8.21 The FBI is the lead federal agency for responding to threats from weapons of mass destruction (WMD). The Bureau investigates and collects intelligence on WMD-related threats and incidents to prevent attacks and respond to them when they occur.

A WMD is defined as:

1. Any explosive (see the following list), incendiary, or poison gas
 - a. Bomb
 - b. Grenade
 - c. Rocket having an explosive or incendiary charge of more than 4 ounces
 - d. Missile having an explosive or incendiary charge of more than 1/4 ounces
 - e. Mine
 - f. Device similar to any of the devices just described
2. Any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors
3. Any weapon involving a disease organism
4. Any weapon that is designed to release radiation or radioactivity at a level dangerous to human life

8.3 Terror, Threats, Disaster, and Intelligence Agencies

The FBI provides support nationally to agencies of government at the state, local, and federal levels in the prevention, containment, and detection of WMDs. The mission of the WMD Directorate is essentially fourfold:

- **Preparedness:** The WMD Preparedness subprogram incorporates elements of planning, training, and exercises to ensure that the FBI and its U.S. government partners are ready to respond to WMD threats when they emerge.
- **Countermeasures:** The WMD Countermeasures subprogram consists of outreach activities and more specialized coordination called *tripwires*.
- **Investigations and operations:** The FBI has multiple entities and programs in place around the world for the investigative, intelligence, CI, and overall law enforcement response to a terrorist threat or incident in the United States.
- **Intelligence:** The basis for the FBI's proactive approach to the countermeasures, investigations, and operations is timely, relevant, and actionable intelligence analysis (Figure 8.22).

Education is an increasingly important function of the FBI in all matters relating to homeland security. In the area of WMDs, the FBI takes a special interest. See the mock exercise on a dirty bomb in Figure 8.23.

Internet Exercise: Watch the training video produced by the NSB for local and state law enforcement at <https://youtu.be/TpnbWFJvMpl>.

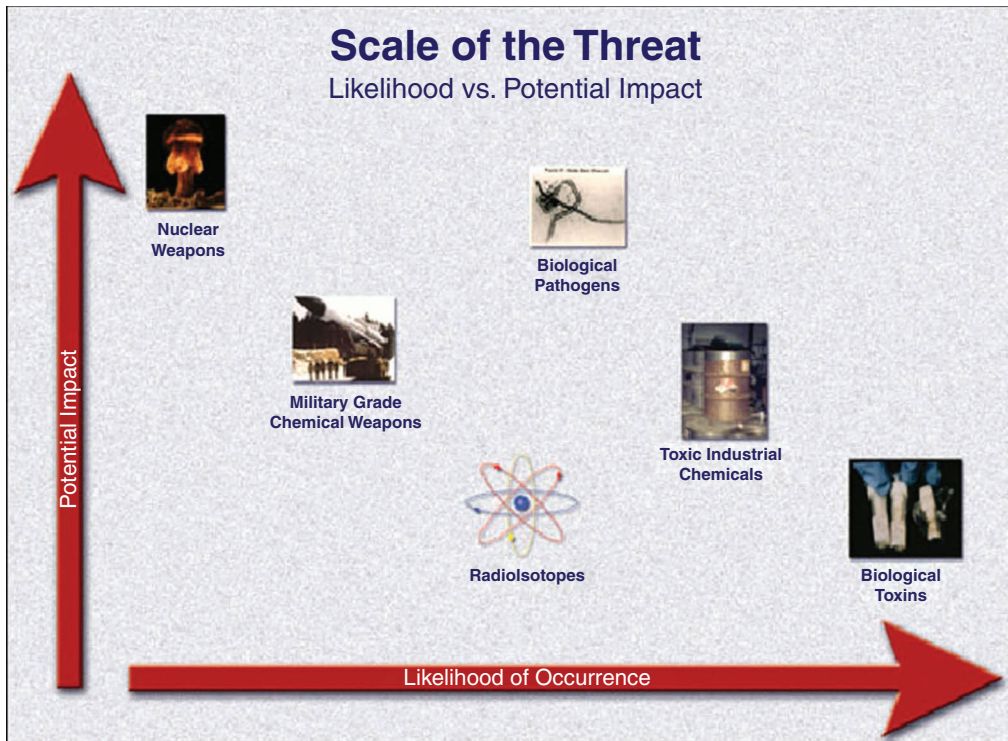


Figure 8.22 Scale of the threat: Likelihood vs. potential impact.

PREPARING FOR DISASTER

How to Respond to a Dirty Bomb



An FBI SWAT team member is checked for possible radiological contamination. The event was part of a staged drill at the Orange Bowl in Miami to show the basics of how we'd respond to a threat involving a weapon of mass destruction. See more images below.

An FBI SWAT team prepares to assault the warehouse.

FBI and Miami Police SWAT teams use paintball weapons to clear the warehouse and capture the terrorist suspects. In the process, they find a mock "dirty bomb" or radiological dispersal device.

If terrorists ever do try to attack our country with a nuke or dirty bomb, the FBI and its partners must be ready.

And we are. On Wednesday, we staged a mock drill at the Orange Bowl in Miami to show the basics of how we'd respond to a threat involving a weapon of mass destruction.

In the scenario, a terrorist cell was in the process of constructing a dirty bomb in a mock warehouse set up on the field at the Orange Bowl. Two Special Weapons and Tactics (SWAT) teams—one from the FBI and one from the Miami Police—descended on the scene, cleared the warehouse, and discovered an improvised explosive device in one room and radiological material in another room. A Department of Energy Radiological Assistance Program Team used sensors to help determine the presence of radiation, and, with the help of the Miami Fire Department, a robot later destroyed the device. Then, an FBI Hazmat team in full protective gear collected radiological evidence at the scene.

The drill came on day three of the FBI's week-long event, the "Global Initiative to Combat Nuclear Terrorism Law Enforcement Conference." Delegates from 28 countries observed the demonstration from the press boxes and later saw equipment and displays showing the WMD capabilities of 15 local, state, and federal agencies.



A member of the FBI Hazardous Materials Response Team uses a long pole to safely collect evidence related to the dirty bomb.



A Miami police robot like this one destroyed an improvised explosive device with streams of water during the exercise.

Figure 8.23 How to respond to a dirty bomb.

8.3.2 Central Intelligence Agency

Since 1947, the CIA has been a central figure in the collection and assessment of data and intelligence (Figure 8.24).

Spawned during the era of the Cold War, the agency, like so many of its fellow agencies, has had to apply its skill and knowledge in the intelligence sector, but carrying out its mission in light of terror and threats to the homeland. In 2004, President George W. Bush restructured the CIA by including a new Office of the Director of the CIA and a Director of National Intelligence—an office that oversees intelligence nationally and coordinates the activities of the National Counterintelligence Office.²⁹ The mission and core values of the agency are as follows:

Service: We put Nation first, Agency before unit, and mission before self. We take pride in being agile, responsive, and consequential.

Integrity: We uphold the highest standards of lawful conduct. We are truthful and forthright, and we provide information and analysis without institutional or political bias. We maintain the Nation's trust through accountability and oversight.

Excellence: We bring the best of who we are to everything we do. We are self-aware, reflecting on our performance and learning from it. We strive to give our officers the tools, experiences, and leadership they need to excel.

Courage: We accomplish difficult, high-stakes, often dangerous tasks. In executing mission, we carefully manage risk but we do not shy away from it. We value sacrifice and honor our fallen.

Teamwork: We stand by and behind one another. Collaboration, both internal and external, underpins our best outcomes. Diversity and inclusion are mission imperatives.

Stewardship: We preserve our ability to obtain secrets by protecting sources and methods from the moment we enter on duty until our last breath.³⁰

In recent years, the agency has undergone a mission re-examination, primarily prompted by new political leadership and priorities. Under President Obama, the vision of every agency had changed. The tendency to seek less confrontation and more conciliation with our former and present enemies has resulted in agencies, such as the CIA, stressing an altered mission that is less aggressive and more collaborative with the world community. This is evident in the revised mission. But that outlook had again been modified under a more aggressive, vision of President Trump. It remains to be seen the approach that the Biden administration takes thought it is anticipated that it will likely be closer to Obama policies than Trump's.



Figure 8.24 CIA Director: Gina Haspel: seventh Director and First Female Appointment: May 21, 2018.

Homeland Security

The CIA is primarily a covert intelligence community. Its methods and means are distinct from traditional law enforcement, yet despite these differences, the need for collaboration and meaningful lines of communication became quite clear on September 11, 2001. The 9/11 Commission Report caustically critiqued the lack of communication lines between the CIA and FBI.³¹

The CIA is organizationally arranged into seven parts:

- Directorate of Analysis
- Directorate of Operations
- Directorate of Science and Technology
- Directorate of Digital Innovation
- Directorate of Support Mission Centers
- Offices of the Director

See Figure 8.25.³²

8.3.2.1 Directorate of Analysis

In the intelligence section, the bulk of what the CIA has refined and honed matters of data collection and interpretation finds a home. Of all the Directorates, there is nothing more compelling related to the work of the CIA. Officers in the CIA's Directorate of Analysis anticipate and quickly assess rapidly evolving international developments and their impact, both positive and negative, on U.S. policy concerns. The intelligence support and findings are disseminated to a specific audience in need of those findings. The President's Daily Brief and the World Intelligence Review (WIRe) are examples of this intelligence reporting.

The Directorate of Analysis contains myriad officers and offices dedicated to the collection, assessment, and dissemination of intelligence.

- The CIA Crime and Narcotics Center collects and analyzes information on international narcotics trafficking and organized crime for policymakers and the law enforcement community.
- The CIA Weapons, Intelligence, Nonproliferation, and Arms Control Center provides intelligence support aimed at doing all it can to protect America from the strategic threat of foreign weapons.
- The Counterintelligence Center Analysis Group identifies, monitors, and analyzes the efforts of foreign intelligence entities against U.S. persons, activities, and interests.
- The Information Operations Center Analysis Group evaluates foreign threats to U.S. computer systems, particularly those that support critical infrastructures.
- The Office of Asian Pacific, Latin American, and African Analysis studies the political, economic, leadership, societal, and military developments in Asia, Latin America, and Sub-Saharan Africa.
- The Office of Collection Strategies and Analysis provides comprehensive intelligence collection expertise to the DI, a wide range of senior agency and intelligence community officials, and key national policymakers.
- The Office of Corporate Resources oversees support to the directorate on a wide variety of issues, including budget, contracts, diversity programs, equal employment opportunity, facilities management, human resources, and resource planning.
- The Office of Iraq Analysis provides multidisciplinary intelligence analysis on Iraq to the president and his top advisors.



Figure 8.25 An overview of the various directorates of the CIA.

Homeland Security

- The Office of Near Eastern and South Asian Analysis provides policymakers with comprehensive analytic support on Middle Eastern and North African countries, as well as on the South Asian nations of India, Pakistan, and Afghanistan.
- The Office of Policy Support customizes DI analysis and presents it to a wide variety of policy, law enforcement, military, and foreign liaison recipients.
- The Office of Russian and European Analysis provides intelligence support on a large number of countries that have long been of crucial importance to the United States as allies or as adversaries and are likely to continue to occupy a key place in U.S. national security policy.
- The Office of Terrorism Analysis is the analytic component of the CIA Counterterrorism Center.
- The Office of Transnational Issues applies unique functional expertise to assess existing and emerging threats to U.S. national security and provides the most senior U.S. policymakers, military planners, and law enforcement with analysis, warning, and crisis support.

Internet Exercise: Find out about careers in the Directorate of Analysis, see <https://www.cia.gov/offices-of-cia/intelligence-analysis/careers-1>

8.3.2.2 Directorate of Operations: Clandestine Services

Clandestine operations connote many images—some forbidden, others unapproved or denied upon discovery. That is a fair assessment, since to be clandestine is, minimally, to be secretive. That the United States has engaged in clandestine operations is really no secret at all. From the failed Bay of Pigs invasion to operating secret prisons for terrorists, the CIA has been a prime player in these covert activities. The agency and its supporters make no apologies for it either. Secret operations are not only essential in the protection of a country, but mandatory. Complex targets such as terrorism prompt complicated responses. Operating within the CIA is the National Clandestine Service (NCS), which conducts specialized operations for the purpose of gathering intelligence and ensuring U.S. security.

Internet Exercise: Find out about the very generous CIA Internships in Clandestine Services at <https://www.cia.gov/careers/student-opportunities/ncs-intern.html>

The CIA references the NCS as a body that collects “information not obtainable through other means.”

Internet Exercise: For once-classified operations now unclassified regarding covert, clandestine operations of the CIA, see <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/index.html>.

8.3.2.3 Directorate of Science and Technology

The Directorate of Science and Technology supports the CIA’s mission by its expertise in technological and scientific applications. Intelligence requires the highest levels of equipment and protocol. Clandestine operations require cutting-edge equipment and technology. The mission of the directorate is to fashion and invent tradecraft that aids the operatives of the CIA and to create and develop technical collection systems, and to apply enabling technologies to the collection, processing, and analysis of information. The Directorate of Science and Technology includes the men and women of the CIA who apply their expertise and training in pure science—applied engineering, master craftsmanship, operational tradecraft, and linguistics—to provide U.S. decision makers with critically important intelligence on the world (Figure 8.26).

8.3.2.4 Directorate of Digital Innovation

The Directorate of Digital Innovation (DDI) is the CIA’s office dedicated to the protection of the nation’s IT structure and what it terms *cyber tradecraft*. Realizing that threats are both real



Figure 8.26 CIA's Directorate of Science and Technology.

and virtual, the directorate advances the most sophisticated technology and protocols to thwart cyber threats that are very real and very meaningful. In this directorate, the CIA looks for evidence of threat and terror by scanning the remnants and shadows of illegal activity capturable in the digital realm. This same office shall be the center for a CIA too long laden with old and insecure equipment across its many offices.

In addition to its overall mission to expand digital and cyber capabilities across the CIA, the new DDI will create a strategic framework to manage the CIA's digital architecture and talent, enhancing the capabilities of the agency's existing directorates and new Mission Centers. The DDI will encourage CIA leadership to aggressively implement innovation in the digital realm and oversee the career development of the agency's digital and cyber experts.

8.3.2.5 Directorate of Support

The Support to Mission team provides mission-focused support to the CIA through a full range of services. The office is responsible for building and operating facilities; providing robust, secure communications over multiple networks, connecting officers sitting in dispersed locations; and acquiring and shipping a full range of critical equipment. The Directorate of Support also helps hire, train, and assign CIA officers for every directorate, as well as manage the “businesses” within the CIA—contracts and acquisitions, financial services, administrative support, and even the CIA's own phone company. The Directorate of Support does everything it can to ensure that CIA officers serving around the world are safe, secure, and healthy.

8.3.2.6 Mission Centers

As part of its overall reorganization and updating, the CIA has erected, aside from some mission tinkering, new mission centers that stress and emphasize particular works and ambitions for the CIA. The mission centers comprise four primary functions for CIA operations and six specifically designated geographic territories.

- Mission Center for Africa
- Mission Center for Counterintelligence
- Mission Center for Counterterrorism
- Mission Center for East Asia and Pacific
- Mission Center for Europe and Eurasia
- Mission Center for Global Issues
- Mission Center for Near East

Homeland Security

- Mission Center for South and Central Asia
- Mission Center for Weapons and Counterproliferation
- Mission Center for Western Hemisphere

Couple this realignment with the agency's stress on modernization and cyber and digital capacity, and it is clear that the CIA underwent a significant transformation during the second term of President Obama. The changes are fully charted in Figure 8.27.

8.3.3 Offices of the Director of National Intelligence

What was painfully obvious to intelligence specialists was the lack of coordination among so many distinct bureaucracies of intelligence.³³ By 2006, it was clear that there were too many cooks in the intelligence kitchen. As a result, President Bush created the ODNI; in some circles, this position is labeled "executive" or "czar." When Congress authorized the creation of the ODNI, it charged the department with diverse authorities and duties, including the following:

- Ensure that timely and objective national intelligence is provided to the president, the heads of departments, and agencies of the executive branch; the chairman of the Joint Chiefs of Staff and senior military commanders; and Congress.
- Establish objectives and priorities for the collection, analysis, production, and dissemination of national intelligence.
- Ensure maximum availability of and access to intelligence information within the Intelligence Community.
- Develop and ensure the execution of an annual budget for the National Intelligence Program (NIP) based on budget proposals provided by intelligence community (IC) component organizations.
- Oversee the coordination of relationships with the intelligence or security services of foreign governments and international organizations.
- Ensure the most accurate analysis of intelligence is derived from all sources to support national security needs.
- Develop personnel policies and programs to enhance the capacity for joint operations and to facilitate staffing of community management functions.
- Oversee the development and implementation of a program management plan for the acquisition of major systems, doing so jointly with the secretary of defense for Department of Defense (DoD) programs, that includes cost, schedule, and performance goals and program milestone criteria.

The idea was to pool all the intelligence resources or to funnel these myriad sources through a central office with a central director. This way one agency could not fail, either inadvertently or intentionally, to withhold intelligence from sister agencies. John Negroponte, a seasoned diplomat and security guru, was the first appointee to this position. Negroponte, by all accounts, skillfully coordinated these diverse constituencies and left the office in high esteem. After President Obama assumed office, Dennis Blair, a former Navy Commander of the Pacific Fleet, whose background includes impeccable experiential and educational preparation, was appointed to the role and served for 2 years. Blair set clear goals for the position, which include the following:

- To serve as the principal intelligence advisor to the president and his national security team. We will continue to enhance the quality of our analysis and the depth and range of collection that supports it. We will integrate contributions from all IC partners, call it

8.3 Terror, Threats, Disaster, and Intelligence Agencies



Figure 8.27 CIA offices organization chart. (<https://www.cia.gov/about-cia/leadership/cia-organization-chart.html>.)

Homeland Security

as we see it, and lay out the alternatives with clear statements of our level of confidence in our judgments.

- To make the whole of the Intelligence Community greater than the sum of its parts. All 17 intelligence organizations can expect clear mission direction. Common areas such as personnel, intra-IC communications, clearances, and classification deserve special emphasis, as do missions that require the capabilities of more than one agency for success. All of us are then accountable for mission success.
- To assess mission and resources and then provide resources adequate to meet assigned responsibilities and build future capabilities.³⁴

During the tenure of Director James R. Clapper, a retired military officer with significant intelligence experience (Figure 8.28), the ODNI and related intelligence services were tied to the investigation of the Trump campaign's collusion with Russia. On August 18, 2020, the Republican-led Senate Intelligence Committee in fact issued a report finding which detailed political coordination among the Trump campaign, Wikileaks, and Russian intelligence and operatives in 2016.

During the Trump Presidency, there were multiple appointments including William Dempsey, Dan Coats, Joseph Maguire, Rich Grinnel, and John Ratcliffe. Avril Haines was sworn in as the Director of National Intelligence on January 21, 2021. She is the seventh Senate-confirmed DNI and the first woman to lead the U.S. Intelligence Community (see Figure 8.29).

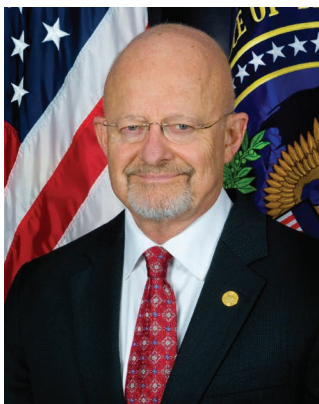


Figure 8.28 James R. Clapper, Director of National Intelligence.



Figure 8.29 Avril Haines: Director of National Intelligence.

8.3 Terror, Threats, Disaster, and Intelligence Agencies



Figure 8.30 Seal of the Office of the Director of National Intelligence.

The mission of the ODNI is multifaceted, but its central aim is the coordination of intelligence information across a host of agencies and operatives (Figure 8.30).

In its strategic statement, the ODNI lists the constituencies that it serves. Turf battles give way to collective cooperation and sound homeland policy. The ODNI holds that intelligence will integrate foreign, military, and domestic intelligence capabilities through policy, personnel, and technology actions to provide decisional advantage to policymakers, warfighters, homeland security officials, and law enforcement personnel. This ambition can only be termed a lofty one, for it properly hopes for the type of sharing and intelligence cooperation that government historically resists. The ODNI has many tools at its disposal. A summary look follows.

Internet Exercise: Visit the ODNI's Electronic Reading Room for a sample of its many findings and reports at <https://www.dni.gov/index.php/foia>.

8.3.3.1 National Counterterrorism Center

The National Counterterrorism Center (NCTC) was created to be a central clearinghouse for integrating and analyzing terrorism information. The NCTC comprises people from its many partner agencies and is a center based on cooperation, collaboration, and partnership. See Figure 8.31.

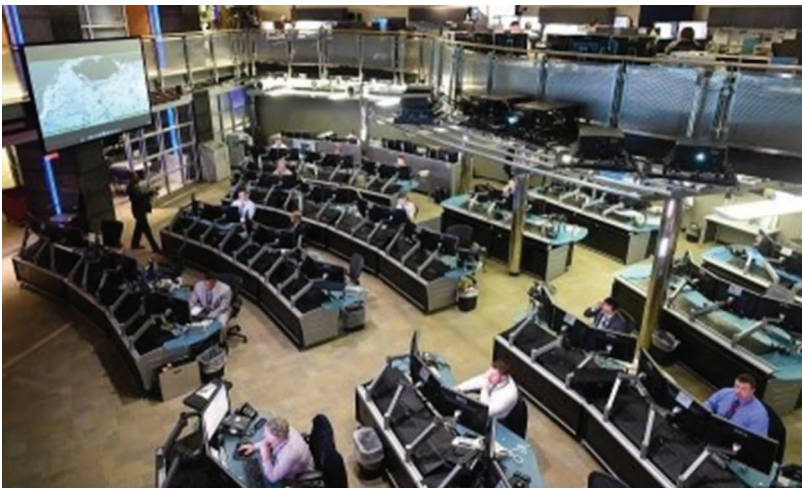


Figure 8.31 NCTC in operation. (Source: NCTC.)



Figure 8.32 Seal of the National Counterterrorism Center.



Figure 8.33 Major Nidal Malik Hasan, the shooter at Fort Hood.

The NCTC seal symbolizes this and, like the design of the great seal of the United States, represents a united center engaged in the global fight against terrorism (Figure 8.32).

A special emphasis of the NCTC is the detection and prediction of domestic activities that threaten the homeland.³⁵ The NCTC has come under some withering criticism for its failure to share intelligence on Major Hasan, the mass murderer at Fort Hood (Figure 8.33).³⁶

Congressional hearings confirmed that the structural difficulties of intelligence sharing and the “wall” between “law enforcement and intelligence”³⁷ still existed nearly a decade later. And this persistent shortfall may be “inevitable”³⁸ given the complexities of the intelligence function. However, it seems a necessary ambition to improve the methods and means by which the NCTC shares its information, as well as how all other intelligence agencies share their knowledge base.

8.3.3.2 National Counterintelligence and Security Center

The Office of the National Counterintelligence Executive (ONCIX) was part of the ODNI and staffed by CI and other specialists. The ONCIX developed, coordinated, and produced

- Foreign intelligence threat assessments and other analytic CI products
- CI strategy for the U.S. government

8.3 Terror, Threats, Disaster, and Intelligence Agencies

- CI policy on collection, investigations, and operations
- CI program budgets and evaluations
- Espionage damage assessments
- CI awareness, outreach, and training standards policies (Figure 8.34)

This office developed the National Intelligence Strategy,³⁹ which lays out broad policies on intelligence and produces recommendations on how to undermine terrorists and terrorism and protect intelligence capabilities.⁴⁰ The office has merged two previous sectors—namely, the Special Security Center and the Center for Security Evaluation, effective 2010. In 2014, the office was reorganized and renamed the National Counterintelligence and Security Center (NCSC) and operates under the full supervision of the ODNI (Figure 8.35).

The business of the NCSC primarily consists of the following duties:

- National Threat Identification and Prioritization Assessment (NTIPA) program and other analytic CI products
- Development of the National Counterintelligence Strategy of the United States

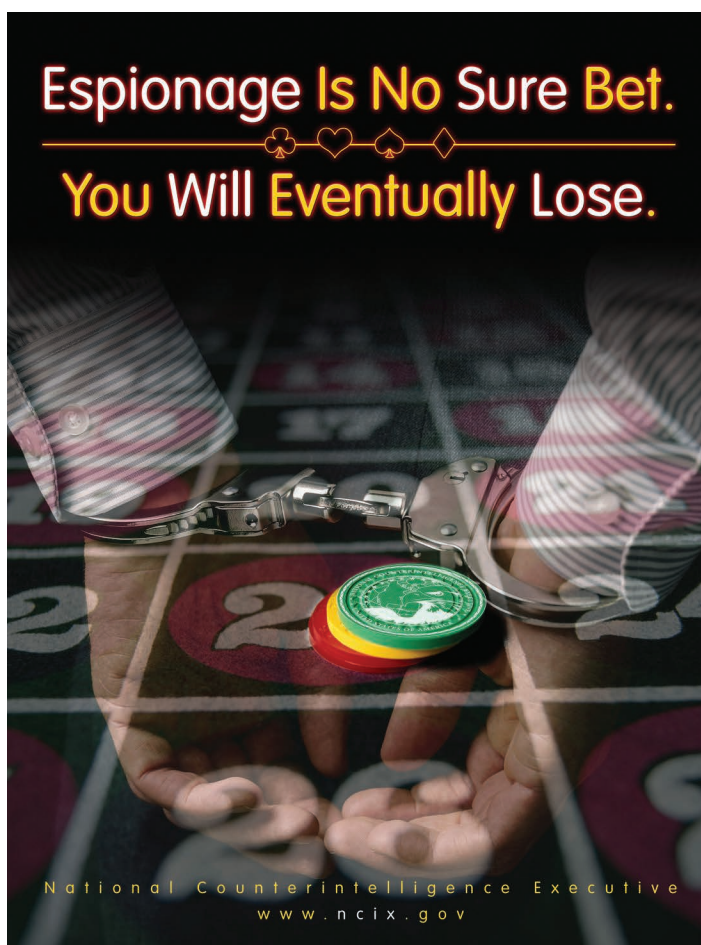


Figure 8.34 The ONCIX poster “Espionage Is No Sure Bet” serves as a reminder that there are no winners in the espionage game.



Figure 8.35 Seal of the NCSC.

- Counterintelligence collection, investigations, and operations
- Espionage damage assessments
- Counterintelligence awareness, outreach, and training standards

Internet Exercise: Read the NCSC's 2020–2022 National Counterintelligence Strategy at https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf

8.3.3.3 National Intelligence Council

The National Intelligence Council (NIC) provides an intellectual and policymaking center for the director of national intelligence. Its core missions are to

- Promote exemplary use of analytic tradecraft and standards, including alternative analysis, new analytic tools and techniques, and wider collaboration within the IC
- Provide senior policymakers with coordinated views of the entire Intelligence Community, including National Intelligence Estimates
- Prepare IC principals and represent the IC at National Security Council principals and Deputies Committee meetings
- Tap non-U.S. government (USG) experts in academia and the private sector to broaden the IC's knowledge and perspectives

The NIC expends a good portion of its energy and time on projections—that is, what it expects the future holds. For terror prevention, the policymaker and homeland professional need to always stay a step or two ahead to succeed. The NIC's projections are short term and long term in design. Its projections to the year 2030 portray a world with the types of problems presently witnessed and a bold projection of emergent issues likely to be encountered.⁴¹ A sample of these projections is reproduced in Figure 8.36.⁴²

The NIC authors the influential National Intelligence Estimates, which comprise the coordinated judgments of the Intelligence Community regarding the likely course of future events. The NIC makes every attempt to stay apolitical in its advice to politicians and policymakers, although the content of the estimate is often used for political reasons. The NIC estimates have been fodder for those opposing the wars in Iraq and Afghanistan, since the pictures drawn in the estimates have not always been complementary to decisions relating to these campaigns. The estimates can ruffle feathers, but at their foundation is the desire of the NIC to deliver objective information on tough security problems.

8.3 Terror, Threats, Disaster, and Intelligence Agencies

Global Trends and Key Implications Through 2035

The rich are aging, the poor are not. Working-age populations are shrinking in wealthy countries, China, and Russia but growing in developing, poorer countries, particularly in Africa and South Asia, increasing economic, employment, urbanization, and welfare pressures and spurring migration. Training and continuing education will be crucial in developed and developing countries alike.

The global economy is shifting. Weak economic growth will persist in the near term. Major economies will confront shrinking workforces and diminishing productivity gains while recovering from the 2008-09 financial crisis with high debt, weak demand, and doubts about globalization. China will attempt to shift to a consumer-driven economy from its longstanding export and investment focus. Lower growth will threaten poverty reduction in developing countries.

Technology is accelerating progress but causing discontinuities. Rapid technological advancements will increase the pace of change and create new opportunities but will aggravate divisions between winners and losers. Automation and artificial intelligence threaten to change industries faster than economies can adjust, potentially displacing workers and limiting the usual route for poor countries to develop. Biotechnologies such as genome editing will revolutionize medicine and other fields, while sharpening moral differences.

Ideas and Identities are driving a wave of exclusion. Growing global connectivity amid weak growth will increase tensions within and between societies. Populism will increase on the right and the left, threatening liberalism. Some leaders will use nationalism to shore up control. Religious influence will be increasingly consequential and more authoritative than many governments. Nearly all countries will see economic forces boost women's status and leadership roles, but backlash also will occur.

Governing is getting harder. Publics will demand governments deliver security and prosperity, but flat revenues, distrust, polarization, and a growing list of emerging issues will hamper government performance. Technology will expand the range of players who can block or circumvent political action. Managing global issues will become harder as actors multiply—to include NGOs, corporations, and empowered individuals—resulting in more ad hoc, fewer encompassing efforts.

Figure 8.36 An overview of global trends by 2030. (From NIC, *Global Trends 2030* (Washington, DC: NIC, December 2012), <http://www.dni.gov/index.php/about/organization/global-trends-2030>. Accessed August 16, 2016.)

(Continued)

The nature of conflict is changing. The risk of conflict will increase due to diverging interests among major powers, an expanding terror threat, continued instability in weak states, and the spread of lethal, disruptive technologies. Disrupting societies will become more common, with long-range precision weapons, cyber, and robotic systems to target infrastructure from afar, and more accessible technology to create weapons of mass destruction.

Climate change, environment, and health issues will demand attention. A range of global hazards pose imminent and longer-term threats that will require collective action to address—even as cooperation becomes harder. More extreme weather, water and soil stress, and food insecurity will disrupt societies. Sea-level rise, ocean acidification, glacial melt, and pollution will change living patterns. Tensions over climate change will grow. Increased travel and poor health infrastructure will make infectious diseases harder to manage.

The Bottomline

These trends will converge at an unprecedented pace to make governing and cooperation harder and to change the nature of power—fundamentally altering the global landscape. Economic, technological and security trends, especially, will expand the number of states, organizations, and individuals able to act in consequential ways. Within states, political order will remain elusive and tensions high until societies and governments renegotiate their expectations of one another. Between states, the post-Cold War, unipolar moment has passed and the post-1945 rules-based international order may be fading too. Some major powers and regional aggressors will seek to assert interests through force but will find results fleeting as they discover traditional, material forms of power less able to secure and sustain outcomes in a context of proliferating veto players.

Figure 8.36 (*CONTINUED*) An overview of global trends by 2030. (From NIC, *Global Trends 2030* (Washington, DC: NIC, December 2012), <http://www.dni.gov/index.php/about/organization/global-trends-2030>. Accessed August 16, 2016.)

The NIC depends on a cadre of national intelligence officers (NIOs), who engage the security questions in an applied sense and gather intelligence both nationally and internationally. Some of the common functions for NIOs are to

- Advise the DNI.
- Interact regularly with senior intelligence consumers.
- Produce top-quality estimates.
- Engage with the outside.
- Help assess the capabilities and needs of IC analytic producers.
- Promote collaboration among IC analytic producers on strategic warnings, advanced analytic tools, and methodologies.

8.3 Terror, Threats, Disaster, and Intelligence Agencies

- Articulate substantive priorities to guide intelligence collection, evaluation, and procurement.

Internet Exercise: Find out about the many careers in this arm of the Intelligence Community at <http://diajobs.dia.mil/>.

8.3.4 Defense Intelligence Agency

The DIA, founded on October 1, 1961, was, for a large part of its history, a combat support agency. The DIA collects and produces foreign military intelligence for the DoD and aligned intelligence agencies. The DIA reports to the defense agencies as well as the national security staff of the president, members of Congress, and military commanders. The DIA directs itself to six main areas: “all-source analysis, human intelligence, CI, a worldwide secure information technology backbone measurements and signatures intelligence.”⁴³ The DIA also operates a fully accredited university, the Defense Intelligence University, which offers undergraduate and graduate programs.

The DIA serves as lead agency for the intelligence needs of the DoD.⁴⁴

Internet Exercise: To find out more about the DIA college, visit <http://ni-u.edu/wp>.

The DIA summarizes its mission, vision, and values as follows:

Mission

Provide intelligence on foreign militaries and operating environments that delivers decision advantage to prevent and decisively win wars.

Vision

Be the indispensable source of defense intelligence expertise.

Values

We are committed to

Teamwork: Partnering at all levels and across organizational boundaries for mission accomplishment.

Integrity: Adherence to the highest legal and ethical principles in our responsibilities.

Excellence: Unrivaled defense intelligence expertise.

Service: Putting the welfare of the Nation and commitment to our mission before oneself.⁴⁵

With nearly 17,000 employees, the DIA is a major player in the world of intelligence. DIA intelligence covers a broad spectrum of topical coverage and includes but is not limited to

- Foreign military and paramilitary forces
- Proliferation of WMDs
- International terrorism
- International narcotics trafficking
- Information operations
- Defense-related foreign political, economic, industrial, geographic, and medical and health issues

DIA is headquartered at the Joint Base Anacostia–Bolling in Washington, DC, with major operational activities at the Defense Intelligence Analysis Center, the National Center for Medical Intelligence in Frederick, Maryland, and the Missile and Space Intelligence Center in Huntsville, Alabama (Figure 8.37).



Figure 8.37 Seal of the DIA at Joint Base Anacostia–Bolling.

Internet Exercise: See the DIA’s salute to its own officers and all of law enforcement on May 14, 2020, at <https://www.dia.mil/News/Videos/>

A major component of the agency, the Defense HUMINT Service, meaning human intelligence, gathers information by traditional face-to-face interaction rather than technical services. The DIA also manages the Defense Attaché System, which has military attachés assigned to more than 135 embassies overseas. In addition to these functions, the DIA operates and coordinates the functions of the Joint Intelligence Task Force for Combating Terrorism (JITF-CT).

Internet Exercise: For a timeline and historical perspective on the DIA, see http://fas.org/irp/dia/dia_history.pdf.

8.4 Conclusion

The idea and concept known as intelligence is the chapter’s chief aim, and how intelligence becomes part of the homeland security mission is a secondary purpose. In intelligence, the homeland professional recognizes that information is the lifeblood of any meaningful operation or policy. Acting quickly upon intelligence led to the successful raid on Osama bin Laden in his Abbottabad, Pakistan compound in the early hours of May 2, 2011 (Figure 8.38).

Without information, and shared distribution of the same, the homeland operative works in the dark in a literal and figurative sense. Intelligence takes the guesswork out of homeland task and function. DHS promotes the integrative approach to intelligence, whereby information is gathered by the various arms of government—namely, the military, federal, state, local, and private sector justice agencies—and friendly information from foreign allies is weighed and evaluated. DHS encourages cooperation among historic competitors in the bureaucratic sense. It calls on agencies of government to shun the traditional turf systems and parochial protection mechanisms that hardly promote a policy of sharing. There are a host of structural obstacles to the sharing of intelligence. DHS devises the TTIC to serve as a central repository for relevant terrorist intelligence.

Additionally, the chapter paints the picture of intelligence agencies that have been part of the historic and contemporary landscape. Predictably, the CIA and its various branches dedicated to intelligence are featured. Special attention is given to the FBI, who’s international thrust and historic responsibility for crimes of terror and espionage provide early expertise in the fight against terrorism. Terrorism would eventually sweep up the agency and consume it in ways it had never originally envisioned. The FBI developed advanced CI systems, the capacity to trace, detect, and prevent attacks by WMDs, and devised and erected the TSC. The FBI is on the



Figure 8.38 President Obama, then Vice President Biden, and then Secretary of State Hilary Clinton with members of the national security team, receive an update on Operation Neptune's Spear, a mission against Osama bin Laden, in one of the conference rooms of the Situation Room of the White House, May 1, 2011. They are watching live feed from drones operating over the bin Laden complex.

forefront of information sharing. The educational role of the FBI in matters of terrorism is also being evaluated. With the FBI working closely with the CIA, the traditional turf protection systems that thwarted the sharing of information will end. Eventually, all agencies will contribute to the NCTC—a clearinghouse of information on threats.

Special attention is given to new agencies that have arisen since the tragedy of 9/11 as well as the reorientation of existing agencies that have had to revise operational missions to contend with the terrorist threat. In particular, the chapter scrutinizes efforts to centralize and coordinate the massive volume of intelligence across a plethora of federal agencies. Here, the ODNI will play a central role. Known as the Office of the Intelligence Czar, the ODNI has become a focal point for intelligence systems. The director oversees a host of intelligence operations and functions, including the NCTC, the ONCIX, and the NIC. Each of these entities carries out critical work in the world of intelligence. Finally, the chapter ends its coverage of the intelligence sector by reviewing the work of the DIA—that crucial collaboration of military and civilian intelligence gathering and sharing. The DIA's more essential contributions to the intelligence theater are highlighted.

Keywords

Change of Mandate; Clandestine Operations; Counterintelligence; Counterterrorism; Covert Intelligence Community; Defense Attaché System; Defense Intelligence Agency; Director of National Intelligence; Directorate of Science and Technology; Espionage; Federal Bureau of Investigation; Global Terrorism; HUMINT; Intelligence Community; Intelligence; Joint Terrorism Task Force; National Clandestine Service; National Counterintelligence Executive; National Counterterrorism Center; National Espionage Estimates; National Intelligence Council; National Intelligence Officers; National Intelligence Strategy; National Security Branch; Office of Support; President's Daily Brief; Terrorist Screening Center; Terrorist Threat Integration Center; World Intelligence Review

Discussion Questions

1. Explain how the FBI had to change its outlook and mission after 9/11. How significant was this reorientation?
2. Previous to 9/11, the FBI stressed what tasks and duties when compared with terrorism?
3. JTTFs assimilate many agencies into the mix. How does this assist in their outlook and work?
4. Evaluate and comment on the CIA's Directorate of Science and Technology. What are its purpose and aim?
5. Discuss the ramifications of an intelligence practice based on a nonshared environment. Why do some argue that 9/11 would never have occurred if information sharing had been commonplace?
6. Explain why cooperation between the military complex and federal intelligence agencies is so important in the fight against terrorism.
7. What types of projections make sense in the intelligence arena? What is a projection worth making?
8. Does it make sense to create an ODNI? Are there alternatives to this design?
9. What do you envision is the greatest challenge for the director of national intelligence?
10. How has the mission of the DIA changed in the last 50 years?

Practical Exercises

1. Find and locate a JTTF in your area. Respond to the following:
 - a. What geographic area does the task force cover?
 - b. Whom or what is eligible to join?
2. Describe at least three initiatives the JTTF is presently undertaking.
3. Watch any training video prepared by the FBI relating to terrorism. State four major findings agreed to after reviewing the media.
4. Search the DIA for career opportunities. Create a form file for these career tracks.
5. Find out about career opportunities for intelligence officers in today's military branches.
6. Visit any of the centers mentioned in this chapter.
7. Visit the CIA's Office of Clandestine Services. Analyze, assess, and critique a current operation relating to homeland security.
8. Prove whether the FBI is correct in concluding that ecoterrorists are a dangerous lot.
9. Identify and create a job file for the following occupations in homeland security:
 - a. Federal Protective Service
 - b. Secret Service
 - c. Border Patrol
 - d. Customs officer

- e. FBI agent
 - f. CIA officer
10. Determine where the closest intelligence center is relative to your residence. Check to determine whether any of the following apply:
- a. Military base
 - b. Fusion center
 - c. JTTF
 - d. Regional Office of State Homeland Security
 - e. Special operations unit

Notes

- 1 See D. Khan, An historical theory of intelligence, *Intelligence and National Security* 16 (Autumn 2001): 87–88; P. Gorman, *Hearings before Select Committee on Intelligence of the United States Senate, S. 2198 and S. 421, 102nd Congress* (Washington, DC: Library of Congress, 1992), 262.
- 2 Congressional Research Service (CRS), T. Masse, editor, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches* (Washington, DC: Library of Congress, 2006), 2, <http://www.fas.org/sgp/crs/intel/RL33616.pdf> (accessed August 18, 2020).
- 3 CRS, R. A. Best, Jr., editor, *Intelligence Issues for Congress* (Washington, DC: Library of Congress, 2011), 5, <http://www.fas.org/sgp/crs/intel/RL33539.pdf> (accessed August 18, 2020).
- 4 See: U.S. Naval War College, Intelligence Studies: Types of Intelligence Collection, <https://usnwc.libguides.com/c.php?g=494120&p=3381426> (accessed August 18, 2020).
- 5 See also C. G. Pernin, L. R. Moore, and K. Comanor, *The Knowledge Matrix Approach to Intelligence Fusion* (Santa Monica, CA: Rand Corporation, 2007).
- 6 See M. Chertoff, Current and Planned Information Sharing Initiatives, Keynote presentation, *SEARCH Symposium on Justice and Public Safety Information Sharing* (Washington, DC, 2006).
- 7 See: G. Harkins, Pensacola Shooter Radicalized Years before Terror Attack on Navy Base, FBI Says, May 19, 2020, Military.com, <https://www.military.com/daily-news/2020/05/19/pensacola-shooter-radicalized-years-terror-attack-navy-base-fbi-says.html> (accessed August 18, 2020).
- 8 CNIC, CNIC Commander Visits NSF at Pensacola, December 13, 2019, https://www.cnic.navy.mil/news/news_releases/cnic-commander-visits-nsf-at-pensacola.html (accessed August 18, 2020).
- 9 See: US Dept of Defense Press Release, January 1, 2020, <https://www.defense.gov/Newsroom/Releases/Release/Article/2049534/statement-by-the-department-of-defense/> (accessed August 18, 2020).
- 10 A. Soufan, Qassem Soleimani and Iran's Unique Regional Strategy, *CTC Sentinel*, 11(10) (November 2018), <https://ctc.usma.edu/qassem-soleimani-irans-unique-regional-strategy/> (accessed August 18, 2020).
- 11 US Dept of Homeland Security, Homeland Security Information Network-Intelligence Fact Sheet, <https://www.dhs.gov/sites/default/files/publications/HSIN-Fact%20Sheet-HSIN-Intel.pdf> (accessed August 18, 2020).
- 12 M. Lowenthal, Transforming intelligence, *American Intelligence Journal*, 29 (2011): 10.
- 13 Homeland Security Act of 2002, P.L. 107–296, *U.S. Statutes at Large*, 116 (2002): 2135.
- 14 The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), P.L. 108–458, *U.S. Statutes at Large*, 118 (2004): 3638.
- 15 E. Berman, Regulating domestic intelligence collection, *Washington and Lee Law Review*, 71 (2014): 3.
- 16 US Department of Homeland Security, I&A Organization Chart, https://www.dhs.gov/sites/default/files/publications/18_0817_ia_organizational-chart.pdf (accessed August 18, 2020).
- 17 See: US Drug Enforcement Administration, Intelligence webpage, <https://www.dea.gov/intelligence> (accessed August 18, 2020).
- 18 Federal Bureau of Investigation, What We Investigate webpage, <https://www.fbi.gov/investigate> (accessed August 18, 2020).

Homeland Security

- 19 Naylor, Brian; Lucas, Ryan (March 2, 2021). "Watch: Wray Stresses Role of Right-Wing Extremism In Hearing About Jan. 6 Riot". NPR. Retrieved March 2, 2021.
- 20 Federal Bureau of Investigation website, <http://www.fbi.gov> (accessed August 18, 2020).
- 21 See: FBI, State Department Partner with Kenya to Launch First Overseas Joint Terrorism Task Force, February 10, 2020, *Homeland Security Today*, <https://www.hstoday.us/subject-matter-areas/counterterrorism/fbi-state-department-partner-with-kenya-to-launch-first-overseas-joint-terrorism-task-force/> (accessed August 18, 2020).
- 22 See: FBI News, A New Partnership with Kenya: Training the First Overseas Joint Terrorism Task Force, February 10, 2020, <https://www.fbi.gov/news/stories/first-overseas-jttf-to-be-established-in-kenya-021020> (accessed August 18, 2020).
- 23 Federal Bureau of Investigation website, <http://www.fbi.gov> (accessed August 18, 2020).
- 24 FBI, National Joint Terrorism Task Force, <https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces> (accessed August 18, 2020).
- 25 DHS, *Fusion Centers and Joint Terrorism Task Forces*, <https://www.dhs.gov/fusion-centers-and-joint-terrorism-task-forces> (accessed August 18, 2020).
- 26 FBI, National Security Branch, About page, <https://www.fbi.gov/about/leadership-and-structure/national-security-branch> (accessed August 18, 2020).
- 27 FBI, National Security Branch organizational chart, <https://ucr.fbi.gov/nsb/nsb-org-chart> (accessed August 18, 2020).
- 28 see: US FBI, Office for Victim Assistance, Law Enforcement and the National Security Branch: A Partnership To Protect America, (2006), <https://www.ncjrs.gov/App/publications/Abstract.aspx?id=238912> (accessed August 18, 2020).
- 29 CRS, R. A. Best, Jr., editor, *Intelligence Issues for Congress* (Washington, DC: Library of Congress, 2011), 20, <http://www.fas.org/sgp/crs/intel/RL33539.pdf> (accessed August 18, 2020).
- 30 See CIA, About the CIA webpage, <https://www.cia.gov/about-cia/cia-vision-mission-values> (accessed August 18, 2020).
- 31 P. S. Roberts, How security agencies control change: Executive power and the quest for autonomy in the FBI and CIA, *Public Organization Review*, 9 (2009): 169–198.
- 32 CIA, Office of the CIA sheet, https://www.cia.gov/about-cia/todays-cia/Offices_of_CIA.pdf (accessed August 18, 2020).
- 33 ODNI fact sheet, February 24, 2017, https://www.dni.gov/files/documents/FACTSHEET_ODNI_History_and_Background_2_24-17.pdf (accessed August 18, 2020).
- 34 ODNI, Letter of Dennis C. Blair to employees, January 30, 2009, http://www.governmentattic.org/14docs/ODNIcongCorres_2009-2010.pdf (accessed August 18, 2020).
- 35 National Counterterrorism Center, Domestic Terrorism Conference Report, https://www.dni.gov/files/2020-01-02-DT_Conference_Report.pdf (accessed August 18, 2020).
- 36 CRS, R. A. Best, Jr., editor, *The National Counterterrorism Center (NCTC): Responsibilities and Potential Congressional Concerns* (Washington, DC: Library of Congress, 2011), 8–9, <http://www.fas.org/sgp/crs/intel/R41022.pdf> (accessed August 18, 2020).
- 37 Ibid at 9.
- 38 Ibid at 10.
- 39 See ONCIX, *The National Counterintelligence Strategy of the United States*, 2009.
- 40 Finding out exactly who the enemy may be is always a challenge, even in the case of Al Qaeda. See M. L. Hummel, Who is running Al Qaeda? *The Homeland Security Review*, 5 (2011): 1.
- 41 NIC, *Global Trends 2025: A Transformed World* (Washington, DC: U.S. Government Printing Office, November 2008), iv, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf (accessed August 18, 2020).
- 42 See Office of the Director of National Intelligence, Paradox of Progress, <https://www.dni.gov/index.php/global-trends/trends-transforming-the-global-landscape> (accessed August 18, 2020).
- 43 R. C. Ackerman, Honing defense intelligence, *Signal* (October 2011): 47.
- 44 See: Defense Intelligence Agency, Strategic Approach (September 2018), https://www.dia.mil/Portals/27/Documents/About/DIA_Strategic_Approach.pdf (accessed August 18, 2020).
- 45 Defense Intelligence Agency, Leadership webpage, <http://www.dia.mil/About/Leadership/> (accessed August 18, 2020).

Border Security, U.S. Citizenship, and Immigration Services

OBJECTIVES

1. To identify the various government agencies and their offices that are responsible for securing America's borders
2. To outline the history of what is now Customs and Border Protection (CBP)
3. To explain the various programs of CBP for securing our borders from the illegal entry of immigrants
4. To summarize the programs that CBP has initiated to facilitate the efficient processing and securing of cargo in ports across the globe
5. To outline the history of what is now the U.S. Citizenship and Immigration Services (USCIS)
6. To summarize the various policies and law that has been enacted relative to immigration since the 1920s
7. To explain the mission, policies, and procedures of USCIS as they relate to illegal immigration and terrorism
8. To summarize the programs that USCIS has developed in response to the threat of terrorism

9.1 Introduction

The task of protecting the nation's borders constitutes a major core competency for those involved in homeland security. It is an astounding responsibility with coverage areas that are almost impossible to compute. The sheer size of American geography makes the task overwhelming, though with increasing usage of technology and aircraft tools, our borders are dramatically improving (Figure 9.1).

And since the beginning of the Trump Presidency, efforts to control by physical means, such as wall or fencing, have been a tough road due to Congressional resistance as well as the human



Figure 9.1 A portal observation tower that is gaining popularity on the border.

caravans moving up from Central America. To say this has been contentious is an understatement. See Figure 9.2.

Internet Exercise: Visit Re-imagining Migration to understand the issues around the migrant caravan back in 2018: <https://reimaginingmigration.org/talking-and-teaching-about-the-fall-migrant-caravan/>

9.2 U.S. Customs and Border Protection

Since 1924, a Border Patrol office has been responsible for making our territorial lines secure, but much has changed since the early days of border protection. In recent years, the Border Patrol has become increasingly occupied with mass migrations as well as immigrants. Both tasks are very challenging. The Border Patrol, as a result of the events of 9/11, was merged into the Department of Homeland Security (DHS) and then further aligned with its historic partner, Customs.¹ Customs has an even longer history than the Border Patrol. Originally established as a revenue collector with the founding of the United States in 1776, Customs evolved into much more than the revenue machine it continues to be today. Customs has primary oversight on questions of cargo, duties, and revenue enforcement; trade and environmental law questions;



Figure 9.2 Honduran refugee caravan. A new migrant caravan: 2,000 Honduran migrants traveling toward Mexico. (October 21, 2018. Creative Commons Public Domain Mark 1.0.)

imports and exports; and cargo and port issues. The range and breadth of responsibilities simply impress.

On a typical day in 2019, the CBP

- Processed:
 - 1,124,075 passengers and pedestrians
 - 371,912 incoming international air passengers and crew
 - 70,414 passengers and crew on arriving ship/boat
 - 681,750 incoming land travelers
 - 273,338 incoming privately owned vehicles
 - 78,703 truck, rail, and sea containers
 - \$7.3 billion worth of imported goods
- Conducted 2,354 apprehensions between U.S. ports of entry
- Arrested 23 wanted criminals at U.S. ports of entry
- Encountered 790 inadmissible persons at U.S. ports of entry
- Intercepted 18 fraudulent documents
- Discovered 314 pests at U.S. ports of entry and 4,695 materials for quarantine - plant, meat, animal by-product, and soil
- Seized:
 - 3,707 pounds of narcotics; disrupted 109 pounds of narcotics
 - \$207,356 undeclared or illicit currency
 - \$4.3 million worth of products with Intellectual Property Rights violations

Homeland Security

- Collected approximately \$224 million in duties, taxes, and other fees, including more than \$197 million in duties
- Facilitated the release of 97,342 entries of merchandise at air, land, and seaports of entry
- Employed 61,506 men and women including law enforcement and trade personnel:
 - 24,511 CBP officers
 - 2,465 CBP agriculture specialists
 - 19,648 Border Patrol agents
 - 597 air interdiction agents (pilots)
 - 339 marine interdiction agents
 - 296 aviation enforcement agents
 - 979 trade personnel
- Deployed 1,411 canine teams and 278 horse patrols
- Flew 202 enforcement hours at and beyond the border, and within the nation's interior
- Underway 66 float hours of enforcement missions in the U.S.
- Conducted operations in:
 - 52 countries with more than 1,700 CBP employees working internationally
 - 328 ports of entry within 20 field offices
 - 135 Border Patrol stations within 20 sectors including 35 immigration checkpoints
 - 74 Air and Marine Operations locations, including branches and units, National Air Security Operations Centers, and the Air and Marine Operations Center²

Today, DHS delegates the integrity of our land border to a newly formed entity within DHS—the U.S. CBP program. CBP is responsible for guarding 7,000 miles of land border the United States shares with Canada and Mexico and 2,000 miles of coastal waters surrounding the Florida peninsula and the coast of Southern California. The agency also protects 95,000 miles of maritime border in partnership with the U.S. Coast Guard (Figure 9.3³).

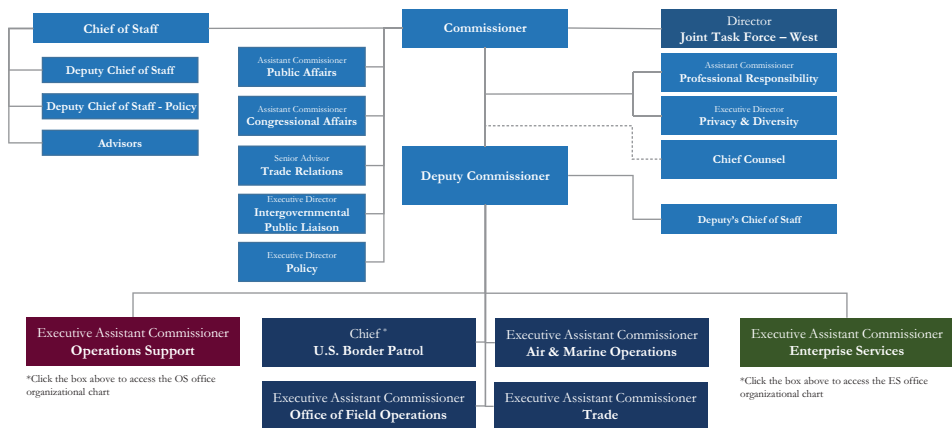
The structure of CBP can be seen in Figure 9.4.⁴



Figure 9.3 The U.S. Coast Guard on border patrol.

9.2 U.S. Customs and Border Protection

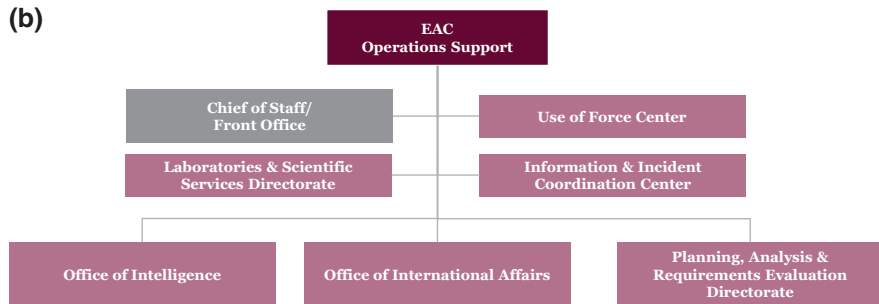
(a)



*Chief of USBP has rank of Executive Assistant Commissioner



(b)



(c)

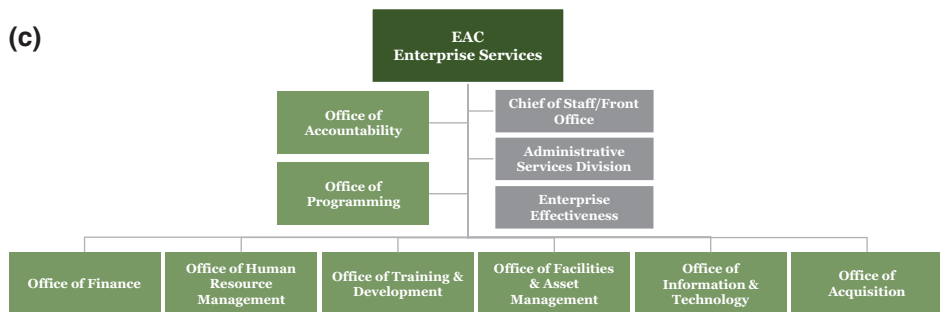


Figure 9.4 CBP organization chart.

Homeland Security

The various departments of CBP manifest the overall mission of the agency—to approach homeland security from two distinct directions. In the first instance, CBP concerns itself with the threat of terrorism and the paths of entry the terrorist may follow into the American landscape, as well as the influx of illegal immigration. In the second instance, CBP, due to its responsibility for cargo, port, commerce, and revenue collection, constantly concerns itself with the intricacies of travel and trade. The agency knows its police role keenly and, at the same time, realizes that it plays a critical role in the movement of goods and services. A closer look at these two missions of CBP follows.

9.2.1 Border Protection

With nearly 7,000 miles of American border, CBP has a serious problem when it comes to ensuring the integrity of our borders. Few issues rile up public debate more than the growing issue of illegal aliens crossing into American territory, even though these individuals are seeking work and a better life. Although, the United States being the “land of opportunity” is not an adage without limitations—especially when our economic circumstances are as challenging as the pandemic causes.

But there are border crossers whose motivations are not economic. Terrorists are now less likely to use commercial aircraft as was done during 9/11 and are more likely to attempt border crossings.. Hence, it is a fact that CBP must concern itself with border protection more than it has historically done. Indeed, since 2004, CBP has reoriented its mission in radical ways and produced some very productive results. For the period 2019–2020, the CPB could only be described as active and in constant service. This data is updated in Table 9.1⁵.

CBP represents the best in adaptation and operational flexibility in government service. At every level of its operation, CBP has targeted its attention on the border while simultaneously honing in on the terrorist. CBP established the National Targeting Center—Passenger (NTC-P) as the centralized coordination point for all of CBP’s antiterrorism efforts (Figure 9.5).

NTC-P also coordinates with other federal agencies, such as the U.S. Coast Guard, Federal Air Marshals, Federal Bureau of Investigation (FBI), Transportation Security Administration, and Departments of Energy and Agriculture. See Figure 9.6.

Immigration and Customs Enforcement (ICE)’s National Security Investigations Division undertakes a wide variety of programs relating to terrorism and defense of the homeland. Given that borders are a pathway to the homeland, the inescapable reality is that these distinct worlds often collide. Some of the division’s more notable sectors of involvement are as follows:

- *Counter-Proliferation Investigations Program:* The Counter-Proliferation Investigations Program oversees a broad range of investigations related to preventing terrorist groups from obtaining U.S. military technology, weapons of mass destruction, or chemical, biological, radiological, and nuclear materials.
- *Export Enforcement Coordination Center:* The Export Enforcement Coordination Center serves as the primary force within the federal government to coordinate U.S. export control enforcement efforts. The center was created by Executive Order 13558.
- *Counterterrorism and Criminal Exploitation Unit:* The Counterterrorism and Criminal Exploitation Unit investigates nonimmigrant visa holders who violate their immigration status. The unit places the highest priority on monitoring the activities of suspected terrorists and combating criminal exploitation of the nation’s student visa system.
- *Human Rights Violators and War Crimes Unit:* The Human Rights Violators and War Crimes Unit pursues foreign war criminals, persecutors, and human rights abusers who seek shelter from justice in the United States.

Table 9.1 CBP Enforcement Statistics Fiscal Year 2020						
Total CBP Enforcement Actions		FY17	FY18	FY19	FY20 TD JUN	
Office of Field Operations (OFO)						
Total encounters		216,370	281,881	288,523	189,885	
U.S. Border Patrol						
Total encounters		310,531	404,142	859,501	262,780	
Total enforcement actions		526,901	683,178	1,148,024	452,665	
Search and Rescue Efforts		FY19 TD JUN		FY20 TD JUN		
U.S. Border Patrol—Southwest border only		3,796		3,284		
		FY19 TD JUN		FY20 TD JUN		
Air and Marine Operations—Nationwide		153		97		
Arrests of Individuals with Criminal Convictions or Those Wanted by Law Enforcement		FY17	FY18	FY19	FY20 TD JUN	
Office of Field Operations						
Criminal aliens ^c encountered		10,596	11,623	12,705	6,431	
NCIC ^d arrests		7,656	5,929	8,546	5,249	
U.S. Border Patrol						
Criminal aliens ^c encountered		8,531	6,698	4,269	1,824	
Criminal aliens with outstanding wants or warrants		2,675	1,550	4,153	1,746	
Office of Field Operations Nationwide Currency Seizures						
	FY15	FY16	FY17	FY18	FY19	FY20 TD JUN
Amount (USD)	\$75,964,824	\$62,101,328	\$65,002,856	\$63,691,464	\$68,879,080	\$56,705,458
(Continued)						

(Continued)

Table 9.1 (Continued) CBP Enforcement Statistics Fiscal Year 2020							
U.S. Border Patrol Nationwide Currency Seizures							
	FY15	FY16	FY17	FY18	FY19	FY20 TD JUN	
Amount (USD)	\$4,741,288	\$7,924,537	\$5,869,004	\$7,176,142	\$6,805,695	\$7,504,248	
Office of Field Operations Nationwide Drug Seizures							
	FY 14	FY 15	FY 16	FY 17	FY 18	FY 19	FY20 TD JUN
Cocaine	45,323	38,346	52,838	62,415	51,592	89,207	29,302
Heroin	4,356	6,023	4,224	3,398	5,205	5,427	3,451
Marijuana	438,146	602,821	516,122	366,627	299,419	289,529	256,506
Methamphetamine ^e	19,613	25,495	33,086	46,247	57,440	68,585	103,917
Fentanyl	n/a	70	596	1,875	1,895	2,545	2,034
U.S. Border Patrol Nationwide Drug Seizures							
	FY 14	FY 15	FY 16	FY 17	FY 18	FY 19	FY20 TD JUN
Cocaine	4,554	11,220	5,473	9,346	6,550	11,682	9,540
Heroin	606	518	566	953	568	808	411
Marijuana	1,922,545	1,538,307	1,294,052	861,231	461,030	266,882	204,661
Methamphetamine	3,930	6,443	8,224	10,328	11,314	14,434	10,259
Fentanyl	n/a	n/a	105	181	388	226	392



Figure 9.5 CBP's National Targeting Center.



Figure 9.6 President Trump at NTC on February 2, 2018. (Courtesy of DHS.)

- *National Security Integration Center*: The National Security Integration Center focuses on federal and interagency partner coordination through its three sections. The center's Interagency Strategic Coordination Section works with the Department of Defense to provide operational, technical, and intelligence support.
- *National Security Unit*: The National Security Unit combines the Homeland Security Investigations (HSI)'s national security and counterterrorism efforts into a single force. The unit has oversight of all counterterrorism investigations within ICE and works

Homeland Security

directly with the National Security Council and ICE senior leadership to carry out interagency policy.

- *Overstay Analysis Unit:* The Overstay Analysis Unit identifies visitors who violate their immigration status by overstaying their authorized period of admission. The unit also researches violator records from the Arrival and Departure Information System.
- *National Security Liaisons:* National Security Liaisons are senior HSI personnel who coordinate investigative activity under assignments to various federal agencies and departments. As part of the National Security Investigations Division, liaisons are essential to establishing partnerships and developing close and cooperative working relationships with HSI's partner agencies.
- *Student and Exchange Visitor Program:* The Student and Exchange Visitor Program manages information on foreign students and exchange visitors in the United States. The program uses the Student and Exchange Visitor Information System to monitor schools, active nonimmigrant students, exchange visitors, and dependents approved to participate in the U.S. education system.

Despite all these advances, CBP cannot forget its fundamental mission of securing the border—in both a physical and an intelligence sense.⁶ In other sections within this chapter, programs of border protection are featured.⁷ The more prominent initiatives of CBP will be briefly covered.

9.2.1.1 Secure Border Initiative: Its Creation and Demise

The Secure Border Initiative (SBI) is a comprehensive multiyear plan to secure America's borders and reduce illegal migration. When first announced in 2005, SBI was thought to be only a few years away from full implementation.⁸ The goals of SBI included, but were not limited to

- More agents to patrol our borders, secure our ports of entry, and enforce immigration laws
- Expanded detention and removal capabilities to eliminate “catch and release”
- A comprehensive and systemic upgrading of the technology used in controlling the border, including increased manned aerial assets, expanded use of drones and other unmanned aerial vehicles (UAVs) (Figure 9.7), and next-generation detection technology



Figure 9.7 CPB Drone.

9.2 U.S. Customs and Border Protection

- Increased investment in infrastructure improvements at the border, providing additional physical security to sharply reduce illegal border crossings
- Increased interior enforcement of our immigration laws, including more robust worksite enforcement

As the last few years have shown, these dynamic ambitions were at best naive especially when the overall issue of immigration itself has yet to be fully tackled: “SBI was meant to be the enforcement component to some sort of substantive immigration reform, which has yet to take place.”⁹ SBI was driven by various interests: first, the very real danger of illegal entry by terrorists, and second, the increase in illegal immigrants, the latter of which results in significant social impacts, including strains on health, education, and other systems.

Despite SBI’s intentions, the prime aim to erect a fence worthy of defense has been nothing more than a pipedream. Probably nothing contributes to this incompetency more than our political leaders posturing and arguing about the sensibility of a virtual fence or other barrier in the first place. In Democratic quarters, a select group of political leaders call for no fences or walls, virtual or otherwise, while their counterparts advocate a virtual and physical fence that cannot be scaled. Across this chasm, SBI simply flounders and becomes ripe for the misallocation of resources so common to its overall mission. SBI, despite all good intentions, was cancelled in 2012 due to technological issues. However, SBI suffers from the current dysfunction so evident in our political infrastructure.

Illegal immigration represents a significant challenge for law enforcement too. To put the issue into perspective, the Pew Research Center estimated that the number of illegal immigrants in the United States in 2017 was 10.5 million individuals (Figure 9.8).¹⁰

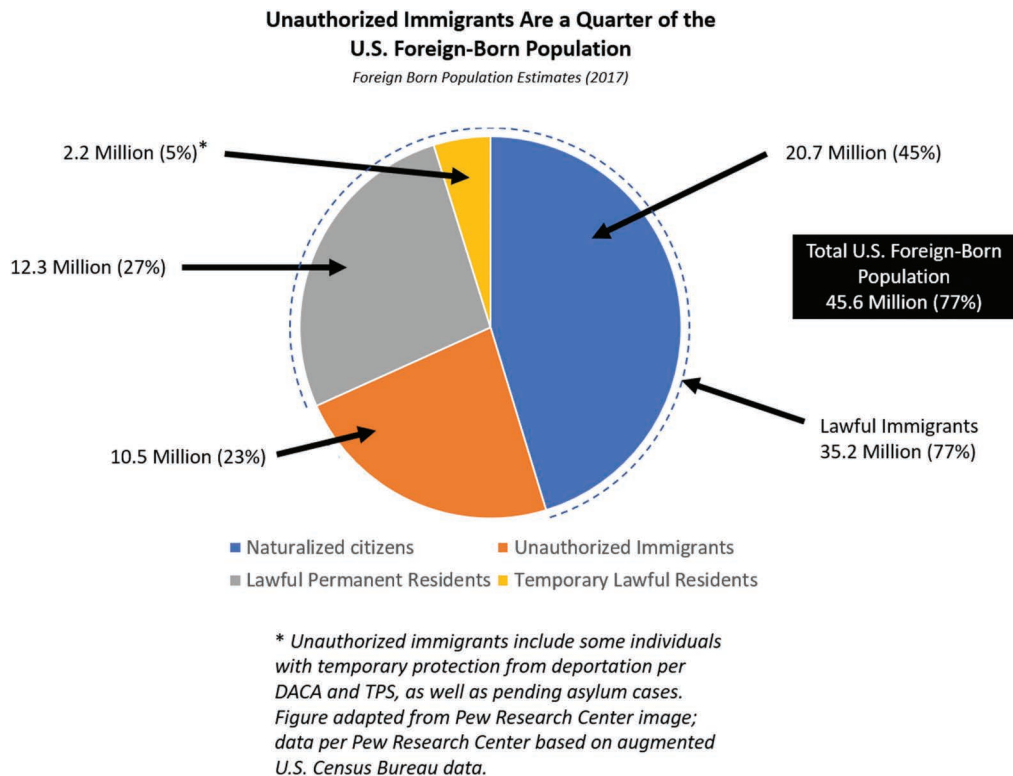


Figure 9.8 Statistics on unauthorized immigrants as a percentage of the total U.S foreign-born population. (Adapted from Pew Research Center.)

Homeland Security

The sheer volume of illegal immigrants over the last three decades has caused operational consternation and frustration at the highest levels of ICE, CBP, and Border Patrol. Even points of entry are overwhelmed. At its center, SBI, by use of technology and other tactics that employ virtual means, has sought to minimize illegal immigration by new initiatives and technology.¹¹

The use of surveillance and remote equipment has been greatly enhanced over the last 10 years, yet neither these technologies nor the physical fence itself have been able to stem the influx of illegal crossings completely—though the volume has slightly abated over the last few years. And as the general public knows, Congressional resistance to funding physical barrier has been a rallying cry to halt the pace of its production. While Congress has provided partial funding, it was President Trump’s decision to transfer some defense funding to the wall construction that allowed for some portions of wall to be built.¹²

Internet Exercise: Visit CBP’s border security mission page for an overview of their operations: <https://www.cbp.gov/border-security/air-sea/missions>.

While the clamor to clamp down goes on with predictable regularity, the full resolution of this longstanding problem continues to elude the policymakers. On any given day, large portions of the border infrastructure are under upgrade, with existing facilities being renovated and fence and border barriers constantly under construction or repair across the continental United States. But the results, the General Accounting Office reports, are only partially successful.¹³ The Southwest region of the United States has long been in dire need of perimeter and barrier protection.¹⁴

More than 670 miles of new fence have been installed and a wide array of natural barriers employed to halt the influx of illegal immigrants entering the country. While physical fencing is still heavily relied on, the nature of barriers continues to evolve. Aside from fence, CBP uses

- Vehicle bollards similar to those found around federal buildings
- “Post on rail” steel set in concrete with a mesh option
- Steel picket-style fence set in concrete
- Concrete jersey walls with steel mesh
- Normandy vehicle fence consisting of steel beams to thwart vehicular attacks (Figure 9.9)



Figure 9.9 Higher Normandy fencing.

9.2 U.S. Customs and Border Protection

There is little question that the Trump Administration had often spoken with a big stick on the question of illegal crossings, migrant caravans, and enforcement. Nor does it help that many of the policies were passed on from the Obama administration. At the same time, the Trump Administration has tried to partner with countries that serve to fill up the caravans—whether Mexico, El Salvador, or Nicaragua. See Figures 9.10 and 9.11.¹⁵

However, it is undeniable that the number of apprehensions and concerted efforts to protect our border are way up. The Pew Research Center charts the Southwest border with upward, escalating data. See Figure 9.12.¹⁶

Internet Exercise: To find out more on the Southwest border fence, visit <https://www.cbp.gov/border-security/along-us-borders/border-wall-system>.

Border protection also employs natural barriers such as rivers, streams, ravines, mountains, cliffs, and other natural artifices to deliver security. Rivers make exceptional barriers, though illegal aliens have long mastered the art of crossing them.

Aside from physical fencing, border protection now relies on the virtual world of fence and barrier. With the rise of technology and the sophistication of surveillance equipment, it is now possible to detect a border crossing and then detach border units within seconds even in the absence of physical fencing. The use of canines has significantly increased as well and with particular success in matters of drug interdiction.¹⁷ The rise in personnel at the border has been astronomical in the last decade (Figures 9.13 and 9.14). Recent efforts have been to funnel more border visitor to points of entry where there is a reasonable infrastructure to deal with both the legalistic and humanistic challenges inherent in the crush of people trying to gain access to the United States. On top of this, the points of entry have facilities that are far better than jumping fence. See Figure 9.15.

Since 2004, the amount of Border Patrol officers has risen 85%, with nearly 20,000 officers on the ground. See Figure 9.16 for a graphical representation.



Figure 9.10 Acting DHS Secretary McAleenan and Minister Hill signed two more key arrangements as part of the regional, comprehensive approach to irregular migration on September 20, 2019. (Source: DHS.)

Homeland Security

GUATEMALA	HONDURAS	EL SALVADOR
		
Border Security Arrangement (Guatemala Arrangement on Irregular Migration): Signed: May 31, 2019 "Memorandum of Cooperation between the Department of Homeland Security of the United States of America and the Ministry of Government of the Republic of Guatemala on Security Activities that Make it Possible to Address Irregular Migration"	Asylum Cooperative Agreement: Signed: Sept. 25, 2019 "Agreement between the Government of the United States and the Government of the Republic of Honduras for Cooperation in the Examination of Protection Claims"	Asylum Cooperative Agreement: Signed: Sept. 20, 2019 "Agreement between the Government of the United States and the Government of the Republic of El Salvador for Cooperation in the Examination of Protection Claims"
*H2A Agreement: Signed: June 30, 2019 "Agreement between the United States of America and the Republic of Guatemala concerning a Temporary Agricultural Workers Program"	Border Security Arrangement: Signed: Sept. 27, 2019 "Memorandum of Cooperation between the Department of Homeland Security of the United States of America and the Ministry of Government of the Republic of Honduras on Security Activities that Make it Possible to Address Irregular Migration"	Border Security Arrangement: Signed: Oct. 28, 2019 "Memorandum of Cooperation between the Department of Homeland Security of the United States of America and the Ministry of Justice and Security of the Republic of El Salvador on Security Activities that Make it Possible to Address Irregular Migration"
Asylum Cooperative Agreement: Signed: July 26, 2019 "Agreement between the Government of the United States and the Government of the Republic of Guatemala on Cooperation in the Examination of Protection Claims"	Biometrics Data Sharing Program Arrangement: Signed: Sept. 27, 2019 "Memorandum between the Government of the United States of America and the Government of the Republic of Honduras on Enhancing Border Security through the Exchange of Information"	Biometrics Data Sharing Program Arrangement: Signed: Oct. 28, 2019 "Memorandum between the Government of the United States of America and the Government of the Republic of El Salvador on Enhancing Border Security through the Exchange of Information"
Biometrics Data Sharing Program Arrangement: Signed: Aug. 22, 2019 "Memorandum between the Government of the United States of America and the Government of the Republic of Guatemala on Enhancing Border Security through the Exchange of Information"	*H2A and H2B Agreement: Signed: Sept. 27, 2019 "Agreement Concerning the Temporary Agricultural and non-Agricultural Workers Programs" <i>*Note: These agreements were signed between the U.S. Department of Labor and Honduras, not DHS.</i>	

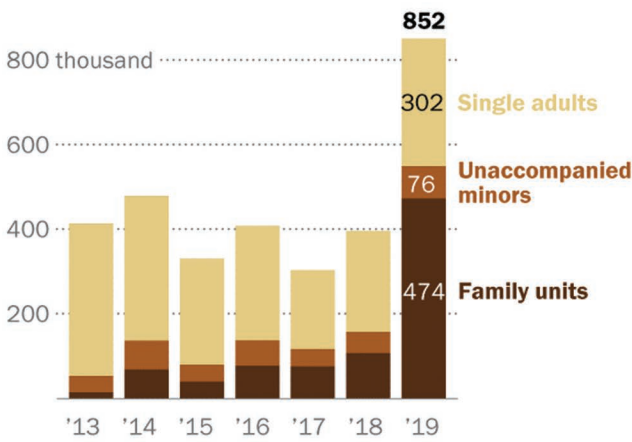


Figure 9.11 Fact sheet on DHS agreements with three central American countries.

Despite this dramatic investment, any plan of securing our border must consider practices and policies above and beyond traditional law enforcement. It has been the historic mission of the Border Patrol to identify, detect, and detain illegal immigrants. Accepting this as a continuing responsibility of any plan of homeland security is not debatable. However, change and innovation need to take the forefront in the homeland defense, and law enforcement alone will not be able to carry out this basic task. Congress and DHS fully understood that law enforcement, in an exclusive sense, would be incapable of securing our borders. Hence, with the merger of Customs and Border, and with the decision to integrate these functions into DHS, CBP looks

Southwest border apprehensions more than doubled in 2019, driven by increase in families

Apprehensions at U.S.-Mexico border, by fiscal year and type



Note: “Family units” refers to the number of people traveling in families.
Source: U.S. Customs and Border Protection.

PEW RESEARCH CENTER

Figure 9.12 Southwest Border Crossing Data per U.S. Customs and Border Patrol. (Adapted from Pew Research Center.)



Figure 9.13 CBP agent searching the shore near San Diego.



Figure 9.14 CBP officer monitoring surveillance cameras.



Figure 9.15 Aerial view of the temporary housing facility June 26, 2019, in Yuma, Arizona, as part of an ongoing response to the current border security and humanitarian crisis along the Southwest border. (Source: CBP.)

at the border in an eclectic way—far beyond a traditional policing function. But in recent years, the challenges of border patrol have become a jumble of demands—already noted, the illegality of entry, the path for the terrorist, the haven for the drug warlord or gang enterprise. And then there is an extraordinary humanitarian problem where human suffering is undeniable—where families are ravaged along the way, women and children raped by coyote criminals and drug

United States Border Patrol
Border Patrol Agent Nationwide Staffing by Fiscal Year

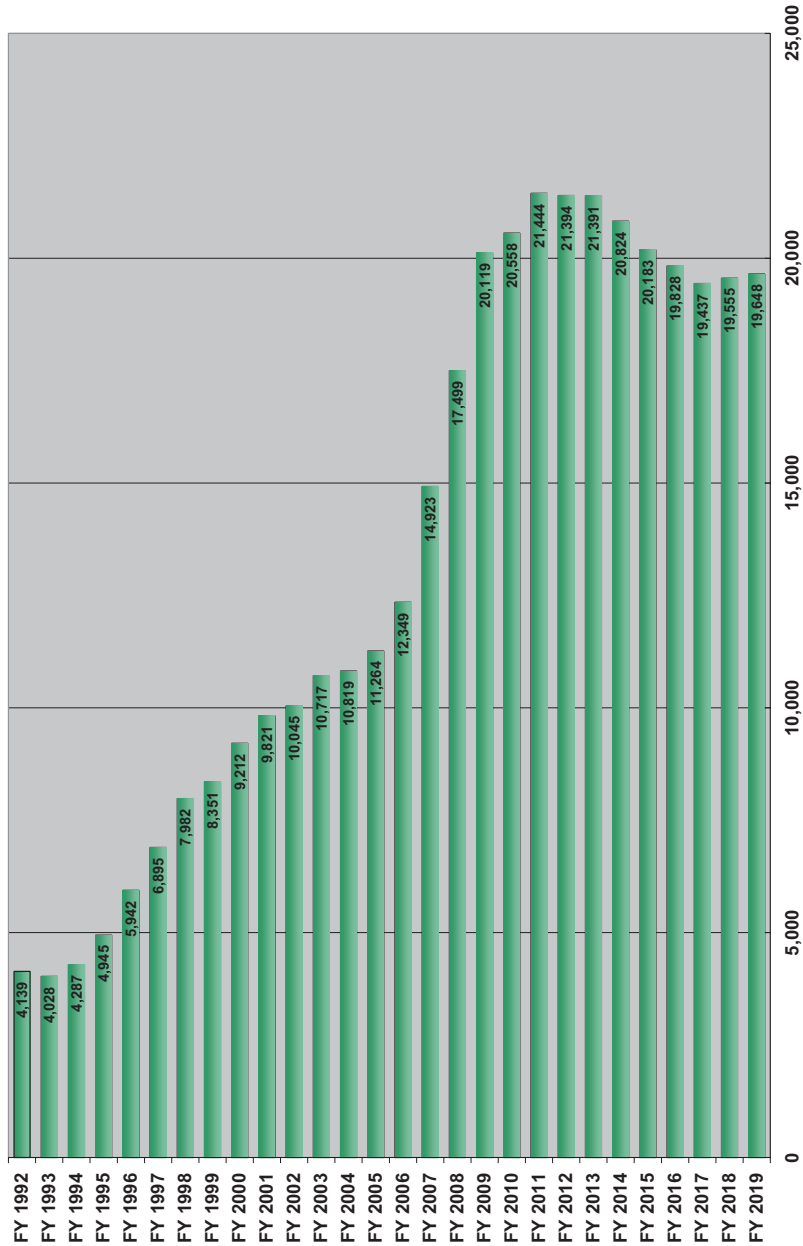


Figure 9.16 Border Patrol agent staffing by fiscal year (as of September 19, 2015). (From CBP, Staffing charts 1992–2014, https://www.cbp.gov/sites/default/files/assets/documents/2020-Jan/U.S.%20Border%20Patrol%20Fiscal%20Year%20Staffing%20Statistics%20FY%201992%20-%20FY%202019%29_0.pdf (accessed January 23, 2016).)



Figure 9.17 Border Patrol Officers at Work. (Source: CBP.)

players. Finally, the system itself simply could not handle the mass of humanity that touched our borderline. No one could have anticipated these numbers and the suffering that was bound to occur when facilities and resources are not more permanent. Entire family units sought entry and that rate rose dramatically from 2018 onward. See Figures 9.17 and 9.18.¹⁸

Yet border protection must constantly and carefully weigh these challenges without forgetting about the threat of the terrorist before issuing any policy. “Terrorists also know that large segments of both the northern and southern border remain relatively unsecured.”¹⁹ Hence, every CBP policy needs to anticipate these dual threats when issuing policy. That analysis must also include new and emerging problems such as massive caravans, gaping holes in the defensive mechanisms hoping to stave off illegal entry and the role of drug cartels, and the “coyote” industry tied to it that barter for illegal entry. The gangs of Mexico often rule in the border towns along the Southwest border and engage in human trafficking.²⁰ CPB has even designed a map which shows their level of influence.²¹ So critical are these gang related and cartel problems that the United States provides economic aid to our law enforcement partners in Mexico whose historic charge of clamping down on these cartels has been beyond challenging.²² So pressing has the border problem been in the last 3 years, that the CBP now trains and works side by side with various military police units. President Trump supported the integration of governmental-military resources because his administration sees the border crush as a crisis that “undermines the integrity of our borders,” and, by extension, U.S. sovereignty.²³ See Figure 9.19.

9.2.1.2 CBP Air and Marine

While CBP expends most of its energies on illegal immigrants coming into America, its mission now rightfully includes the identification, detection, and apprehension of the terrorist, as well as the interdiction of contraband. With the merger of Customs into DHS, its historic mission has shifted to other protection efforts. Realizing this, CBP developed an air and marine (A&M)-based program. The mission of A&M is as follows:

- *Interdiction* encompasses our efforts to intercept, apprehend, or disrupt threats in the land, sea, and air domains as they move toward or across the U.S. borders.
- AMO leverages the expertise of our agents in the air and marine domains to conduct *investigations* to defeat criminal networks.
- *Domain Awareness* is the effective understanding of the environment and information associated with the various domains (air, land, and maritime) that could affect safety, security, the economy, or the environment. AMO employs advance systems to contribute to domain awareness.

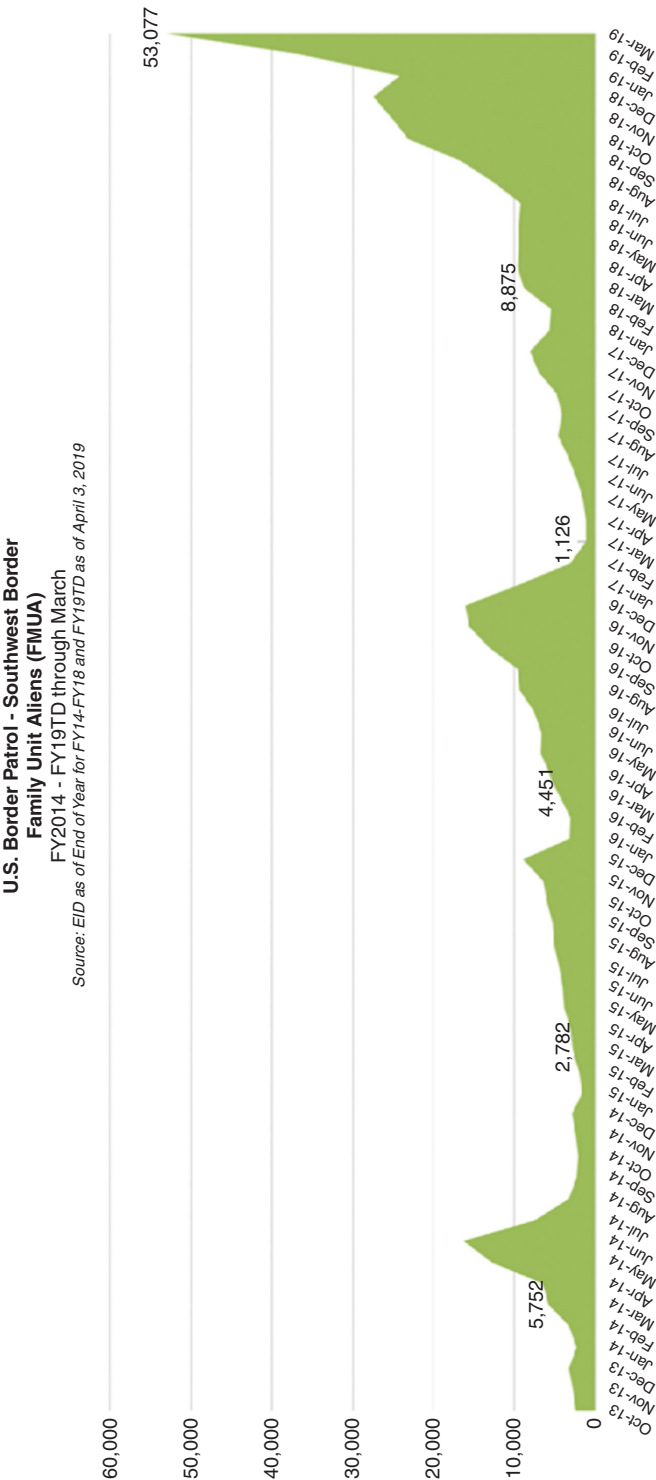


Figure 9.18 Additional Southwest Board statistics as reported by CBP.



Figure 9.19 CBP and Military Police Army Units in 2019 at the Border. (Source: CBP.)

- AMO performs a range of aviation and maritime *contingency operations and national tasking missions*, including Disaster Relief, Contingency of Operations, Humanitarian Operations, Enforcement Relocation, Search and Rescue, and National Special Security Events.²⁴

With nearly 240 aircraft and 300 boat and support vessels,²⁵ CBP is now a major player relative to marine security seeking out illegal activity and potential terrorists at sea (Figure 9.20).²⁶

CBP has developed a law enforcement position, the marine interdiction agent, who is on the front line in the fight against terrorism.

Internet Exercise: To find job announcements for the marine interdiction agent, visit <http://www.usajobs.gov> and search “marine interdiction agent.”

In the air, CBP is just as impressive. To accomplish this mission, CBP A&M utilizes more than 700 pilots and 300 aircraft, including the use of unmanned aircraft systems (UASs). The use of unmanned drones is a critical tool in the fight against terrorism, the interception of drugs, and other illegal activity. The range and breadth of aircraft indicate the seriousness of the CBP purpose in the air. From small propeller planes to Sikorsky helicopters, CBP marshals extraordinary hardware to carry out its mission.²⁷ However, the use of drones, either by governmental entities or private enterprise, is not without risk or difficulties. The CBP has issued warnings about the manufacture of Chinese drones that appear to steal data and intelligence from the US, apart from any potential domestic threats. There are also airspace considerations and private concerns. DHS has charted all the risks and potential downsides in Figure 9.21.²⁸

Internet Exercise: For a thoughtful look at the promise and recurring doubts about drones, see https://www.oig.dhs.gov/assets/pr/2015/oigpr_010615.pdf.

The CBP A&M program greatly increases the productivity and coverage area involved in its mission (Figure 9.22).

The A&M program delivers many services, including:

- Aiding and implementing CBP antiterrorism programs
- Utilizing both manned and unmanned aircraft
- Delivering advanced technology by detection systems
- Providing unrivaled capacity to interdict aircraft, boats, vehicles, and personnel
- Fostering collaborative relationships with law enforcement and the military
- Providing secure airspace



U.S. Customs and
Border Protection

*Coastal Enforcement Class
30-Foot Intrepid*

FACT SHEET



The 30-foot Intrepid coastal enforcement vessel provides a versatile maritime law enforcement capability. The hull design makes it ideal for enforcement operations in shallow, inland and near coastal waters.

The Intrepid meets the demands for a small, fast, highly maneuverable vessel that can be used for interdiction, near coastal and offshore patrol and surveillance.

Marine interdiction agents work together with AMO aviation assets and other federal, state and local law enforcement agencies to accomplish the homeland security mission.

Performance and Weights:

- **Maximum Speed**
46 knots (52 mph)
- **Range**
200 nautical miles (230 miles)
- **Endurance**
Up to 6 hours
- **Length**
30 feet
- **Maximum Gross Weight**
9,500 pounds

Features:

- 2 X 275 HP Mercury outboard engines
- Marine surface radar
- State-of-the-art marine navigational suite

For more information, visit the CBP.gov website
or contact the Office of Public Affairs at (202) 344-1780.

2111-1115

Figure 9.20 Fact sheet for the latest coastal enforcement vessel of the CBP.

9.2.2 CBP and the Facilitation of Trade and Commerce

Along with its partners in the Coast Guard, other military arms, and state and federal law enforcement, CBP assumes essential control and oversight of trade into the American economy—across land, sea, and air. It is not always an easy task, for the policymaker must balance safety and security with the swift and efficient movement of goods. “This becomes a growing challenge in a



EMERGING RISK to INFRASTRUCTURE FROM UNMANNED AERIAL VEHICLES (UAVs)



UAV Capability Versus Policy

ALTITUDE

- Current FAA regulations prescribe a 400 ft. ceiling that is far below the true capability of these devices.
- Current technology devices can reach an altitude of 1,600 ft.
- Cutting-edge technology devices available through retail can climb to an altitude exceeding 15,000 ft.



+15,000 ft



1,600 ft

Current FAA Ruling

Current Technology

Cutting-Edge Technology

RANGE

- FAA regulations require UAV operators keep the device within line of sight—typically within 1,000 ft. of the operator.
- Current technology allows an operator to control a UAV device up to 6 miles.
- Cutting-edge technology allows an operator to control a UAV device up to 13,000 miles.

13,000 miles

6 miles

1,000 ft



GROSS WEIGHT OF DEVICE

- FAA regulations address up to 55 lb. devices.
- Current technology devices weigh approximately 2-8 lbs.
- Cutting-edge technology can weigh 440 lbs.
- 440 lb. devices have a significantly larger payload capacity.
- Payload capacities are being upgraded across a varying range of products at a rapid pace and do not correlate to the gross weight of the device.

55 lbs.

Current FAA Ruling

2-8 lbs.

Current Technology

440 lbs.

Cutting-Edge Technology



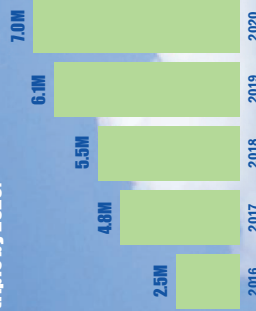
FIRST-PERSON VIEW FLIGHT

- The capability to fly the device based on the view from the UAV itself.
- FAA rulings prohibit this capability.
- The capability is installed on a large number of devices available through retail.

AUTONOMOUS FLIGHT

- The capability for the device to fly itself based on GPS coordinates and preinstalled flight paths.
- FAA rulings do not address this capability.
- Available in many current technology devices.

Number of commercial and hobbyist sales is projected to nearly triple by 2020.

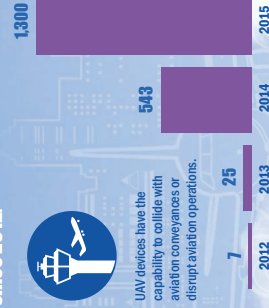


Exposed infrastructure systems and public gathering areas are vulnerable to UAV devices.



- UAVs provide adversaries with the ability to circumvent traditional physical security measures such as gates, surveillance equipment, and security guards.
- Exposed infrastructure systems (such as electrical transmission facilities, pipelines, roads, and bridges) and public gathering areas (such as stadiums and public assembly sites) are vulnerable to UAV devices.

UAV aviation incidents have increased since 2012.



UAV devices have the capability to collide with aviation consequences or disrupt aviation operations.

Figure 9.21 Potential UAV risks to critical infrastructure.



Figure 9.22 CBP patrol plane.

global economy where consumers, just-in-time processes, and integrated supply chains demand reliability, accuracy and speed.”²⁹ The goals of CBP in matters of trade policy are essential to the lifeblood of the American economy. In 2020, the CBP solidified its core purpose and overall goals into three criteria: *Mission, Team and Future*. While these are broad and expansive terms, the CBP has correlated them to specific and particularized activity. See Figure 9.23.³⁰

In addition, Figure 9.24³¹ charts the most recent set of priorities of the CBP in the world of trade and commerce.

Internet Exercise: Find out about this nation’s many ports by using the referenced interactive map at <https://www.cbp.gov/border-security/ports-entry>.

9.2.2.1 Cargo

CBP tracks cargo at various points of entry in the United States. The rules and protocols are quite legalistic, and the agency realizes that the layers of bureaucratic requirements do impact the flow of goods and services on the world market. In a global economy, it is critical that goods and services move expeditiously while at the same time safely and securely. CBP, in conjunction with DHS and other agencies, has implemented some innovative programs relative to cargo. A sketch of the more notable programs follows.

9.2.2.1.1 Secure Freight Initiative

The Secure Freight Initiative (SFI) evaluates capabilities for large-scale radiation scanning of cargo before it ever reaches the United States. Presently, the SFI program is operating at less than a dozen foreign ports with a goal to fully scan all inbound cargo. The stress of the SFI is the nuclear and radiological material that might be employed as WMDs. Port security relies on a multilayered approach to security, best illustrated in Figure 9.25.

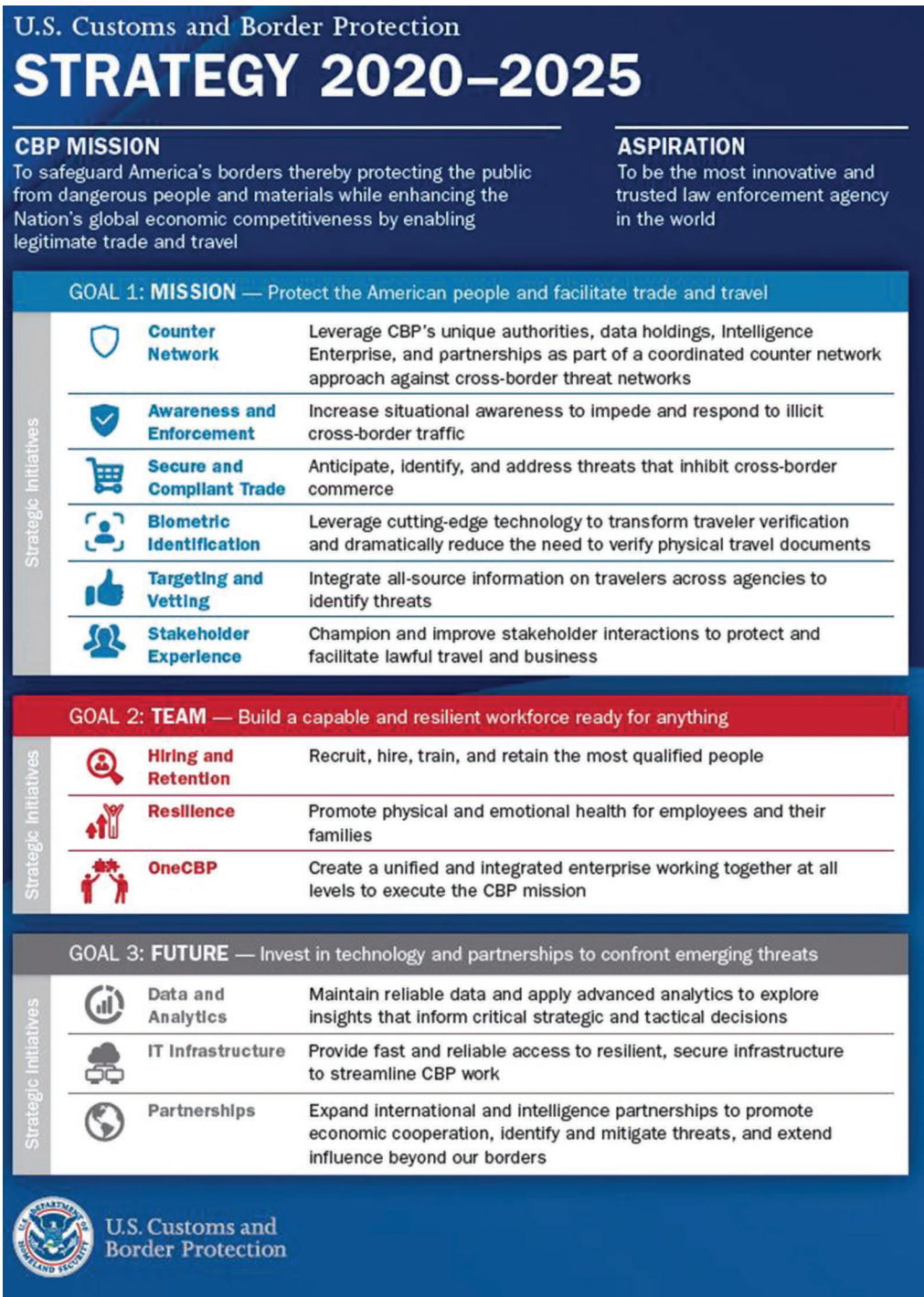


Figure 9.23 U.S. Customer and Boarder Protection’s Strategy through 2025.



Figure 9.24 CBP trade strategy for 2020.

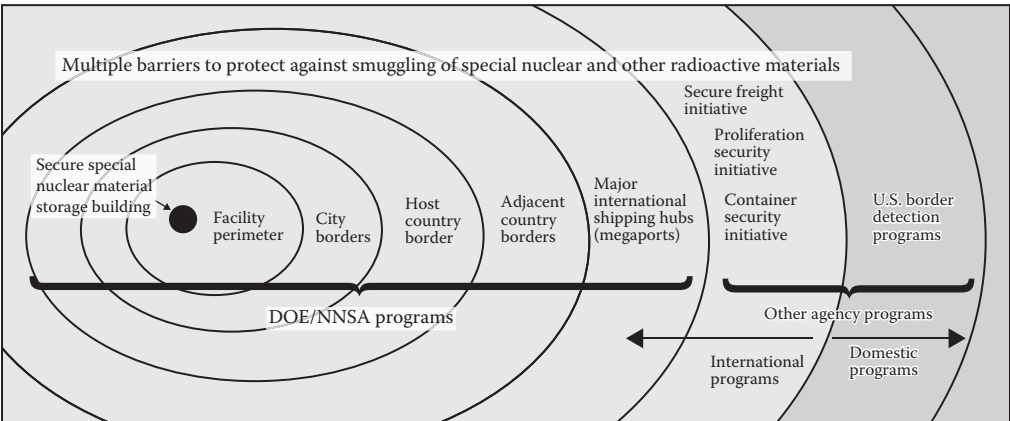


Figure 9.25 DOE/NNSA program combine with DHS and other U.S. and intergovernmental efforts to protect the U.S. homeland against threats from illicit movement of special nuclear and other radioactive materials. (From NNSA, *Megaports Initiative* (September 2010), https://nnsa.energy.gov/sites/default/files/nnsa/inlinefiles/singlepages_9-15-2010.pdf (accessed August 16, 2016).)

Homeland Security

Relying on radiographic equipment, funded by the Department of Energy (DOE)’s National Nuclear Security Administration (NNSA), the SFI uses both active and passive detection systems to scan cargo in large quantities. Passive radiation detection technology includes radiation portal monitors. (See Figure 9.26).

As the cargo and its hold pass through the system, the equipment generates various images by spectrograph, bar graph, infrared, or thermograph reading, as well as traditional x-ray imagery. Radiography uses x-rays or gamma rays to penetrate a container (Figure 9.27).

The SFI tends to favor what are known as *megaports*—that is, locations with huge volumes of cargo. This first phase of the SFI partners with Pakistan, Honduras, the United Kingdom, Oman, Singapore, and Korea, and it will provide these governments with a greater window into potentially dangerous shipments moving across their territory. In Port Qasim, Puerto Cortes, and Southampton, the deployed scanning equipment will capture data on all containers bound to the United States, fulfilling the pilot requirements set out by Congress in the SAFE Port Act³² (Figure 9.28).³³

DHS, NNSA, and DOE have launched a joint screening program that targets megaports using the SFI and the Container Security Initiative (CSI) discussed in the upcoming section, which hopes to identify radiological threats (Figure 9.29).



A seaport container is examined with a mobile truck x-ray

Figure 9.26 Large-scale radiation portal monitors are used to examine cargo. (Source: CBP.)

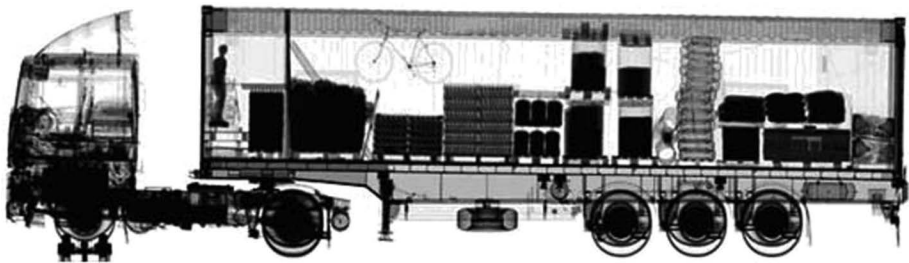


Figure 9.27 X-ray image at an SFI location.



Figure 9.28 SFI scan: A US Customs and Border Protection officer, shakes off his raincoat as he and a fellow officer wrap up scanning of shipping containers as they inspect incoming cargo at the Port of Miami in Miami, Florida.



Figure 9.29 The CSI logo.

The SFI program also operates in selected foreign ports to scan outgoing cargo before leaving port. At the same time, the SFI integrates new data into U.S. government screening and targeting systems, including the proposed new U.S. CBP security filing, as well as the creation of a proposed private sector–operated Global Trade Exchange (GTX). The SFI is testing the feasibility of scanning 100% of U.S.-bound cargo.

9.2.2.1.2 Container Security Initiative

Beginning in January 2002, CBP proposed the CSI, which inspects cargo units rather than the entire freight load and pushes U.S. port security back into the supply chain at its port of origin. The CSI prescreens and evaluates containers before they are shipped. Under the CSI program, high-risk containers receive security inspections by both x-ray and radiation scan. Containers, before being loaded onboard vessels destined for the United States, are inspected at CSI ports. Upon arrival, these same containers are exempt from further inspection, and as a result, goods move through our port system with greater efficiency. The CSI is operational in 58 foreign ports, as shown in Figure 9.30.³⁴

A total of 35 customs administrations from other jurisdictions have committed to join the CSI program.

The CSI now covers 80% of all maritime containerized cargo destined to the United States.³⁵ CSI ports now include

In the Americas:

- Montreal, Vancouver, and Halifax, Canada
- Santos, Brazil

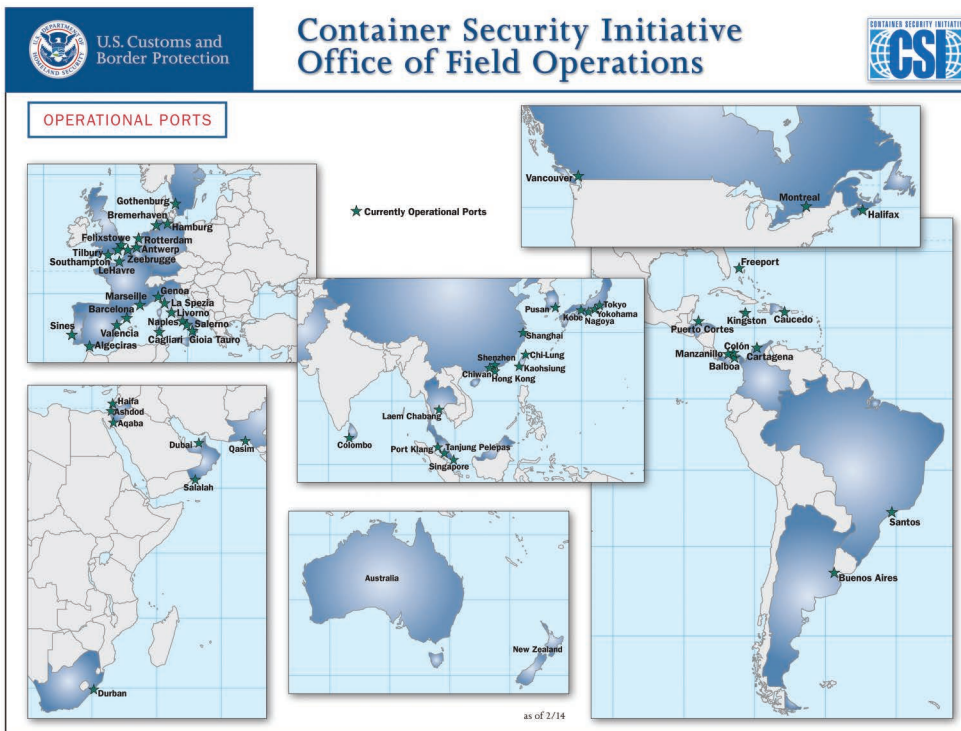


Figure 9.30 CSI operational ports around the world.

- Buenos Aires, Argentina
- Puerto Cortes, Honduras
- Caucedo, Dominican Republic
- Kingston, Jamaica
- Freeport, the Bahamas
- Balboa, Colon, and Manzanillo, Panama
- Cartagena, Colombia

In Europe:

- Rotterdam, the Netherlands
- Bremerhaven and Hamburg, Germany
- Antwerp and Zeebrugge, Belgium
- Le Havre and Marseille, France
- Gothenburg, Sweden
- Cagliari, La Spezia, Genoa, Naples, Gioia Tauro, Salerno, and Livorno, Italy
- Felixstowe, Liverpool, Thamesport, Tilbury, and Southampton, United Kingdom
- Algeciras, Barcelona, and Valencia, Spain
- Sines, Portugal

In Asia and the Middle East:

- Singapore
- Yokohama, Tokyo, Nagoya, and Kobe, Japan
- Hong Kong
- Busan (Pusan), South Korea
- Port Klang and Tanjung Pelepas, Malaysia
- Laem Chabang, Thailand
- Dubai, United Arab Emirates (UAE)
- Shenzhen and Shanghai, China
- Kaohsiung and Chi-Lung, Taiwan
- Colombo, Sri Lanka
- Port Salalah, Oman
- Port Qasim, Pakistan
- Ashdod and Haifa, Israel
- Alexandria, Egypt

In Africa:

- Durban, South Africa

9.2.2.1.3 Customs–Trade Partnership against Terrorism

CBP realizes the essential role that private cargo carriers play in the safety and security of goods flowing through ports and harbors. The Customs–Trade Partnership against Terrorism (C-TPAT) is a voluntary government–business initiative that works closely with the prime players in international cargo—namely, importers, carriers, consolidators, licensed customs brokers, and manufacturers. C-TPAT asks business to ensure the integrity of their security practices and communicate and verify the security guidelines of their business partners within the supply chain. Members must adhere to minimum security requirements with each mode of transport or delivery having unique requirements. C-TPAT members can rely on six regional offices to assist in the event of a security breach or inquiry regarding requirements. The offices are:

- Buffalo, New York ctpatfieldofficebuffalo@cbp.dhs.gov
- Houston, Texas ctpatfieldofficehouston@cbp.dhs.gov
- Los Angeles, California ctpatfieldofficelosangeles@cbp.dhs.gov
- Miami, Florida ctpatfieldofficemiami@cbp.dhs.gov
- New York, New York ctpatfieldofficenewyork@cbp.dhs.gov
- Newark, New Jersey ctpatfieldoffice-newark@cbp.dhs.gov

Internet Exercise: Find out about the many distinct and differing requirements for security in trains, autos, trucks, and other transport at <https://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism/apply/security-criteria>

The goals of C-TPAT are to

- Ensure that C-TPAT partners improve the security of their supply chains pursuant to C-TPAT security criteria

Homeland Security

- Provide incentives and benefits to include expedited processing of C-TPAT shipments to C-TPAT partners
- Internationalize the core principles of C-TPAT through cooperation and coordination with the international community
- Support other CBP security and facilitation initiatives
- Improve the administration of the C-TPAT program

The general theme of C-TPAT is to promote efficiency in the cargo processes and to provide a forum for private–public cooperation in matters of cargo movement. The benefits of C-TPAT are numerous and streamline various inspection processes for cargo and container carriers.

- A reduced number of inspections and reduced border wait times.
- A C-TPAT supply chain specialist to serve as the CBP liaison for validations, security issues, procedural updates, communication, and training.
- Access to the C-TPAT members through the Status Verification Interface.
- Self-policing and self-monitoring of security activities.
- In the Automated Commercial System (ACS), C-TPAT-certified importers receive a reduced selection rate for compliance measurement examinations and exclusion from certain trade-related local and national criteria.
- C-TPAT-certified importers receive targeting benefits by receiving a credit via the CBP targeting system.
- Certified C-TPAT importers are eligible for access to the FAST lanes on the Canadian and Mexican borders.
- Certified C-TPAT importers are eligible for the Office of Strategic Trade (OST)'s Importer Self-Assessment (ISA) program and have been given priority access to participate in the Automated Commercial Environment (ACE) program.
- C-TPAT-certified highway carriers on the Canadian and Mexican borders benefit from their access to the expedited cargo processing at designated FAST lanes. These carriers are eligible to receive more favorable mitigation relief from monetary penalties.
- C-TPAT-certified Mexican manufacturers benefit from their access to the expedited cargo processing on the designated FAST lanes.
- All certified C-TPAT companies are eligible to attend CBP-sponsored C-TPAT supply chain security training seminars.

See Figure 9.31.

Internet Exercise: For an application regarding C-TPAT membership, see <http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism/apply#>.



Figure 9.31 The CTPAT logo.

9.2.2.1.4 Automated Commercial Environment

Modernizing the free flow of goods takes much more than mere personnel and novel policies. The sheer volume of material flowing in and out of the global marketplace demands the highest systems of technology. CBP is upgrading and electronically manifesting the flow of goods through its ACE program. ACE is part of a multiyear CBP modernization effort that is not yet fully operational and is being deployed in phases (Figure 9.32).

ACE seeks to

- Allow trade participants access to and management of their trade information via reports.
- Expedite legitimate trade by providing CBP with tools to efficiently process imports/exports and move goods quickly across the border.
- Improve communication, collaboration, and compliance efforts between CBP and the trade community.
- Facilitate efficient collection, processing, and analysis of commercial import and export data.
- Provide an information-sharing platform for trade data throughout government agencies.

For example, in trucking, relative to cargo and container, the ACE electronic truck manifest capabilities are now available at all 99 U.S. land border ports of entry. Truckers electronically author e-manifests, which provide CBP with cargo information, such as crew, conveyance, equipment as applicable, and shipment details. In ports of entry, there are now mechanisms to file reports and paperwork electronically. As of late 2007, the ACE program was making significant inroads into the cargo and container fabric of America with mandatory e-manifests, the processing of 200,000 trucks per week, faster processing times for e-manifests, the establishment of 14,000 ACE secure data portal accounts, and the collection of nearly 38% of dues and fees computed through electronic periodic reports. In 2015–2016, the ACE program shall impose mandatory usage and participation dates for the program. By the end of the 2016 cargo season, nearly all cargo moving through the American marketplace was subject to the ACE electronic requirements. As of 2020, the ACE program has subsumed nearly all commercial documentation into an electronic format and electronic filing. See the array of services it provides in Figure 9.33.³⁶

The benefits to the ACE program are well documented and include:

- Financial savings with the periodic monthly payment capability
- Reduced processing time at the border with features such as e-manifests



Figure 9.32 ACE program logo.

<i>“I want to...”</i>		ACE via EDI Interfaces	ACE Portal
 Send Importer Security Filing Data *Only low volume through Portal (less than 12 per year)			
 File an Import Air, Ocean, or Rail Manifest			
 File an Import Truck Manifest			
 File an Electronic Inbond			 Via Truck Manifest
 File an Entry			
 File an Entry Summary			
 File a Protest			
 Run Reports			
 Create Blanket Declarations			
 Submit Supporting Documents for Release CBP and PGA Forms		 DIS	
 Submit Supporting Documents for Entry Summary CBP and PGA Forms		 DIS	 Upload Forms
 Respond to Request for Documents CBP Forms 28, 29, 4647		 DIS	
 Manage Account and Periodic Monthly Statement Information			
 Make Post Summary Corrections			
 File Export Air, Ocean and Rail Manifest		<i>Pilots in Progress!</i>	
 File Export Commodity Data			

Figure 9.33 A summary of the various advantages of the ACE program.

- Ability to view shipment status and store data via the ACE secure data portal
- Capabilities to develop over 100 customized reports

See Figure 9.34 for a graphic explanation on the ACE basics.

Internet Exercise: Find out about the new initiatives in the ACE program at <https://www.cbp.gov/trade/automated>

Internet Exercise: Find out about the myriad of training opportunities provided by the CBP and its ACE program at <https://www.cbp.gov/trade/ace/training-and-reference-guides>

9.3 U.S. Citizenship and Immigration Services

Immigration has played an important role in the American experience. Immigrants have a natural home in the newly developed country pre- and post-Revolutionary War. To encourage economic development, immigration was widely supported. In its earliest days, the question of immigration was left to the states. Major ports such as New York and Philadelphia became entry points long before federal involvement. In time, by 1875, the Supreme Court would rule that immigration is a federal responsibility. By 1891, Congress had created the Immigration Service, which foretold and dealt with waves of immigrants during the Industrial Revolution. From 1900 to 1920, nearly 24 million immigrants arrived during what is known as the *Great Wave* (Figure 9.35).

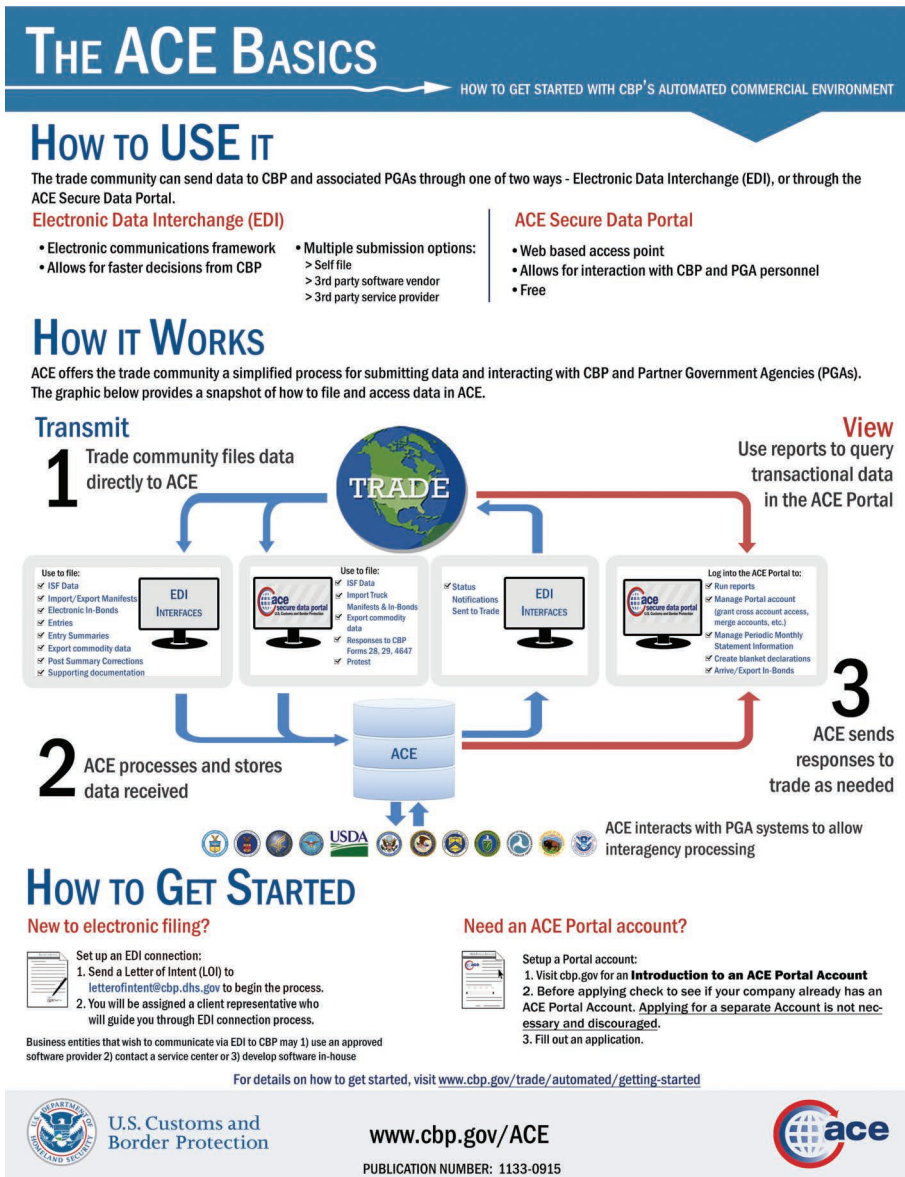


Figure 9.34 The ACE basics: How to get started with CBP's Automated Commercial Environment. (From CBP, The ACE basics, https://www.cbp.gov/sites/default/files/assets/documents/2017-Nov/ACE%20Basics%20-%20November%202017_0.pdf.)

At first, immigration numbers were not limited, but eventually a quota system based on past U.S. Census figures was implemented. In 1924, Congress established the U.S. Border Patrol. For the next three to four decades, the waves of immigrants subsided, but by the 1960s Congress would have to deal with two new constituencies: refugees and transient agricultural workers. Congress passed the Refugee Act of 1980, which delineated U.S. policy on refugees.

Internet Exercise: To see where and when the waves took place, see <http://flowingdata.com/wp-content/uploads/2008/12/21.pdf>.



Figure 9.35 Ellis Island, New York.

In 1986, Congress passed the Immigration Reform and Control Act (IRCA). This legislation had two major eligibility standards: amnesty and enforcement. IRCA provided amnesty to aliens who had completed one of two stipulations: they had resided continually in the United States since January 1982, or they had completed 90 days of agricultural work between May 1985 and May 1986. In 1996, Congress passed the Illegal Immigrant Reform and Immigrant Responsibility Act (IIRIRA). During this same period, various amnesties for illegal immigrants were promulgated. In 1994, Section 245(i) amnesty was enacted, which pardoned 578,000 illegal aliens, who were each fined \$1,000. This amnesty was later renewed in 1997 and again in 2000. The Nicaraguan Adjustment and Central American Relief Act (NACARA) was passed in 1997 and gave legal status to approximately one million illegal aliens, mostly from Central America, who had lived in the United States since 1995. In 1998, the Haitian Refugee Immigration and Fairness Act (HRIFA) passed after it was argued that excluding Haitians from NACARA was discriminatory. The most recent amnesty, passed in 2000, was the Legal Immigration Family Equity (LIFE) Act.

The terrorist attacks on September 11, 2001, provoked a profound re-examination of immigration practices since the terrorists themselves were here as illegal parties. The attack exposed longstanding holes in our immigration system that included failures at visa processing, internal enforcement, and information sharing. Various commissions and other groups have issued reports and recommendations on how improvements might be forthcoming.

In December 2005, the House passed the Border Protection, Antiterrorism, and Illegal Immigration Control Act, which focused on enforcement and on both the border and the interior. Attempts to pass recent legislation granting amnesty to illegals have been widely condemned by public opinion. Various efforts from 2006 to the present regarding immigration reform have faltered.³⁷

Internet Exercise: Find out about the history of immigration in the PowerPoint program developed by the Library of Congress at <https://www.loc.gov/teachers/classroommaterials/presentationsandactivities/presentations/immigration/>.

While issues of immigration frequently touch agencies such as Border Patrol and the Coast Guard, from the prism of law enforcement, there are other issues within the province of USCIS. Once referred to as the Immigration and Naturalization Service (INS), the department was merged into DHS in 2002. USCIS is the primary entity responsible for the administration of immigration status and claims, the adjudication of findings and appeals, and the promulgation of policies and practices concerning the agency. The functions of the agency include, but are not limited to

9.3 U.S. Citizenship and Immigration Services

- Adjudication of immigrant visa petitions
- Adjudication of naturalization petitions
- Adjudication of asylum and refugee applications
- Adjudications performed at the service centers
- All other adjudications performed by the INS (Figure 9.36)

To get the next set of 4 questions, click the generate questions button. When you are ready to review your answers, click the review answers button.

1. What are some of the basic beliefs of the Declaration of Independence?

☐ Freedom of speech, freedom of religion, freedom of the press

☐ That all men are created equal and have the right to life, liberty, and the pursuit of happiness

☐ That there are three branches of government

☐ That there should be checks and balances within the government

2. Who is Commander-in-Chief of the United States military?

☐ The Secretary of State

☐ The Secretary of Defense

☐ The Vice President

☐ The President

3. Where is the White House located?

☐ Camp David

☐ New York City

☐ Virginia

☐ Washington, DC

4. In what month is the new president inaugurated?

☐ July

☐ January

☐ November

☐ June

Figure 9.36 Naturalization self-test.

Homeland Security

The agency is involved in a wide assortment of aligned activities relating to terrorism and potential harm to the United States and its citizens. By its very nature, USCIS has the capacity to be a barrier of entry or a point of forced departure for those intent on doing harm to the United States.

9.3.1 Current Challenges in Immigration

Immigration policy and practice over the last decade have experienced extraordinary challenges, most of which have been covered within this chapter and throughout this entire book. The pressures on our immigration system have never been more intense. The political realities of negotiating an “open” border mentality so often touted by the Democratic Party with the “Build the Wall” argument of Republicans; common ground is tough to find. Add to this, the notion of sanctuary cities, the Visa Lottery where 50,000 people gain entrance into the U.S. by lottery selection, where 800,000 children of illegal immigrants seek citizenship, and the debate becomes even more complex.

9.3.1.1 Sanctuary Jurisdictions

The debate and disagreements about immigration policy have descended into a nearly chaotic state. While immigration law is legislatively a federal question, protected by the alleged theory of federal pre-emption, meaning the sole regulator and overseer of immigration matters should reside and remain at the federal level, certain American states, cities, and counties have formally declared those laws not applicable or relevant to day-to-day immigration policies. It is a movement that has grown substantially over the last 5 years. To see the entire list of jurisdictions, see Appendix C.

The significance of this jurisdictional choice cannot be overstated in the daily lives of ICE officers and agents—whose task it is to detain and arrest those in violation of immigration laws. Many of the potential arrestees have come under the eye and law enforcement scrutiny of state and local law enforcement who were naturally obliged to either notify federal ICE authorities or detain that party if an immigration violation was evident in the record. ICE would even formally send a detainer making the request to hold in confinement for that violation. However, the sanctuary jurisdictions choose not to cooperate.

The issue is highly complex. As the American Immigration Council notes:

Despite the nationwide debate, there is no one clear definition of what it means for a state or local government to adopt sanctuary policies. Sanctuary policies take many forms The common theme behind these categories is that under a sanctuary policy, state and local officials will limit their cooperation with federal immigration officials, but do not actively prevent federal officials from carrying out their immigration enforcement duties.³⁸

And given the absence of a single, agreed-upon definition, UNLV professor of law Michael Kagan points out the local versus federal conundrum:

The discretion that police and prosecutors normally enjoy is complicated by the fact that arrests often have serious collateral consequences, even in the absence of a criminal conviction. If a minor arrest can set into motion a major consequence like deportation, police lose some of their ability to calibrate their policing strategies to the situations they see on the frontlines ... This is complicated terrain for local police to navigate.

Given the wide variety of policies that are categorized under the rhetorical label of sanctuary, there are many different arguments for them. But since immigration enforcement is in the main a federal function, any arguments for local policies should be focused on things over which local and state governments actually have control.³⁹

9.3.1.2 The DACA Dilemma

Closely aligned to the sanctuary mentality is how the DACA program has evolved over the last 6 years. DACA stands for the Deferred Action for Childhood Arrivals—a group of non-citizens who were and are subject to potential deportation. The difficulty is not so much that this group

9.3 U.S. Citizenship and Immigration Services

of about 650,000 are not at fault for simply being the children of those who illegally entered the United States. None of the DACA group was born in the United States, for if they were, citizenship would not be an issue. Instead DACA offspring were born in other countries and simply along for the ride with their parents or guardians when those parties illegally entered the United States. Most people see the difficulty in simply effecting some plan of deportation. The guidelines, as posted by US Customs and Immigration Services were:

You may request DACA if you:

1. Were under the age of 31 as of June 15, 2012;
2. Came to the United States before reaching your 16th birthday;
3. Have continuously resided in the United States since June 15, 2007, up to the present time;
4. Were physically present in the United States on June 15, 2012, and at the time of making your request for consideration of deferred action with USCIS;
5. Had no lawful status on June 15, 2012;
6. Are currently in school, have graduated or obtained a certificate of completion from high school, have obtained a general education development (GED) certificate, or are an honorably discharged veteran of the Coast Guard or Armed Forces of the United States; and
7. Have not been convicted of a felony, significant misdemeanor, or three or more other misdemeanors, and do not otherwise pose a threat to national security or public safety.

9.3.1.2.1 Age Guidelines

Anyone requesting DACA must have been under the age of 31 as of June 15, 2012. You must also be at least 15 years or older to request DACA, unless you are currently in removal proceedings or have a final removal or voluntary departure order, as summarized in the table below:

Your Situation	Age
I have never been in removal proceedings, or my proceedings have been terminated before making my request.	At least 15 years old at the time of submitting your request and under the age of 31 as of June 15, 2012.
I am in removal proceedings, have a final removal order, or have a voluntary departure order, and I am not in immigration detention.	Under the age of 31 as of June 15, 2012, but you may be younger than 15 years old at the time you submit your request. ⁴⁰

As a result, timeframes that allow for continued, or deferred action, was the policy but once the time period for deferral ended, Congress had to legislate a remedy.

Internet Exercise: Review the DACA Toolkit provided by U.S. Customs and Immigration Services at <https://www.uscis.gov/sites/default/files/USCIS/Humanitarian/Deferred%20Action%20for%20Childhood%20Arrivals/DACA-toolkit.pdf>

Since Congress failed to act to extend or modify the deferred status, President Obama, eventually issued an Executive Order by reference to a previous 2012 Order regarding “children” caught in this dilemma. Effective date of this proclamation was June 15, 2012. The legal challenges were immediate since only Congress has the power to legislate regarding immigration status.⁴¹

Homeland Security

During the phases of his Presidency, Donald Trump issued an Executive Order that essentially overturned Obama's DACA policy and proclaimed his lack of legal authority to issue such an Order. Part of the text of that order included:

RESPONSIBLY ENDING UNLAWFUL IMMIGRATION POLICY: Today, the Trump Administration is rescinding the previous Administration's memorandum creating the unlawful Deferred Action for Childhood Arrivals (DACA) program and has begun to end the program responsibly.

- Attorney General Jeff Sessions sent a letter to the Department of Homeland Security explaining that DACA was not statutorily authorized and was therefore an unconstitutional exercise of discretion by the executive branch.
 - Attorney General Sessions found that DACA, given pending litigation, would likely face the same outcome as the Deferred Action for Parents of Americans and Lawful Permanent Residents (DAPA) program, which was enjoined by the courts.
- The Trump Administration is taking responsible action to wind down DACA in an orderly and minimally disruptive manner.
 - If President Trump allowed DACA to go to court, it is likely that the court would abruptly enjoin the program.
 - If President Trump had refused to act, many States were prepared to pursue litigation to end DACA by court order.
 - Under the change announced today, current DACA recipients generally will not be impacted until after March 5, 2018, six months from now. That period of time gives Congress the opportunity to consider appropriate legislative solutions.
- DHS's enforcement priorities remain in place. However, absent a law enforcement interest—which is largely the standard that has been in place since the inception of the program—the Department will generally not take actions to remove active DACA recipients.
 - DACA recipients range from ages 15 to 36, with the overwhelming majority being of adult age.
- Initial requests for Employment Authorization Documents under DACA properly filed and accepted through today will be processed.
 - Additional DACA initial applications filed after today will not be accepted.
- Renewal applications for DACA Employment Authorization Documents properly filed and accepted by October 5, 2017, for people whose current Employment Authorization Documents expire between today and March 5, 2018, will be processed.
 - Any such requests filed after October 5, 2017 will not be accepted.
- Currently approved applications for advance parole for DACA recipients will generally be honored, but new applications will not be approved.
 - All pending applications for advance parole by DACA recipients will be closed and associated fees will be refunded.

RESTORING LAW AND ORDER TO OUR IMMIGRATION SYSTEM: The DACA program was never intended to be permanent—even President Obama admitted it was a temporary, extraordinary measure. And President Obama repeatedly recognized that such unilateral actions were in excess of the Executive's appropriate role.⁴²

Following this decision in September of 2017, various Circuit Court of Appeals and District Courts took up the matter and ruled unfavorably and inconsistently. As a result, the Order was enjoined and, subsequent to the injunction, appealed to the U.S. Supreme Court.

In a ruling the week of June 17, 2020, the Court struck down the Trump Executive Order by a vote 5-4. Chief Justice, John Roberts' opinion stated:

Certain features of the DACA policy may affect the strength of any reliance interests, but those features are for the agency to consider in the first instance. DHS has flexibility in addressing any reliance interests and could have considered various accommodations. While the agency was not required to pursue these accommodations, it was required to assess the

9.3 U.S. Citizenship and Immigration Services

existence and strength of any reliance interests, and weigh them against competing policy concerns. Its failure to do so was arbitrary and capricious.⁴³

And given this narrow conclusion, which critiques a failure to provide a clear rationale for the DACA Order, the Court left open the opportunity and the chance to meet the rule making standard. Read President Biden's Press release, from July 15, 2021 on his plan for immigration reform and DACA: <https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/statement-by-president-joseph-r-biden-jr-on-daca-day/>

9.3.1.3 The Visa Lottery Program

As part of his efforts to stave off immigration the Trump administration sought to end or cut back certain programs. A favorite target has been the Visa Lottery program. The Diversity Immigrant Visa Program (DV Program) makes up to 50,000 immigrant visas available annually, drawn from random selection among all entries to individuals who are from countries with low rates of immigration to the United States. The DV program is administered by the U.S. Department of State (DOS).⁴⁴ See Figure 9.37.⁴⁵

President Trump frequently criticized this program.⁴⁶ He noted in an official White House communique:

CANCELING THE VISA LOTTERY: President Trump has called for the cancelation of the visa lottery system, which selects applicants at random and has been subject to fraud and abuse.

- Currently, about 50,000 immigrants enter the United States each year through the Diversity Immigrant Visa Program, commonly called the visa lottery or Green Card lottery.
- Individuals are selected at random to apply for a visa that permits permanent residence in the United States, and the qualifying criteria are very low.
 - Eligible countries have low levels of immigration to the U.S. over the last 5 years.
 - The program requires participants to have only a high school education or two years of work experience.
- Upon entering the United States, those who have received a Green Card may eventually gain U.S. citizenship through naturalization.
- The visa lottery has been highly vulnerable to fraud and abuse.
 - A 2003 report by the State Department's Office of the Inspector General (OIG) found the visa lottery system is subject to widespread abuse.
 - A 2007 report by the Government Accountability Office (GAO) found the program was vulnerable to fraudulent activity.⁴⁷

The program has been subject to criticism since its selection process has little if anything to do with the merit of the applicant and all the more to do with random selection. While the Trump Administration was highly critical of the program, there was no legislative consensus reached on its revision or its elimination.

9.3.1.4 The Complexity of Chain Migration

Another challenge under current immigration policy has been the growth of immigration triggered by chain migration. Chain migration occurs when a recent migrant, who is legally present, seeks to bring extended family members into the country.⁴⁸

This multiplicative effect drives numbers at a pace that government assistance, schools, medical care, and employment opportunities simply cannot keep up with. The pressures to provide all the resources necessary for the humane treatment of incoming immigrants, and just as importantly, the care and feeding of our own citizenry, are an increasing challenge.

At the same time, America is a place which most of the world long's for. While chain migration is not a new concept and has been a method or technique of gaining access to the United States since the days of Ellis Island, the Trump administration has made concerted and vigorous efforts to end chain migration.⁴⁹



2021 DIVERSITY VISA (DV) PROGRAM INSTRUCTIONS

U.S. Department of State | Bureau of Consular Affairs

Follow the steps below to complete your Diversity Visa Program entry. Read the full instructions carefully prior to starting your application at dvlottery.state.gov.

1

READ THE INSTRUCTIONS.
DV 2021 Instructions can be found at travel.state.gov.

2

FILL OUT & SUBMIT APPLICATION.
Enter between noon on October 2, 2019 and noon on November 5, 2019. Applications can be submitted online at dvlottery.state.gov, (multiple entries will be disqualified).

3

KEEP YOUR CONFIRMATION NUMBER.
Make sure you keep the confirmation number at the end of your entry and don't share it with anyone.

4

ENTRANT STATUS.
Check if you were selected starting May 5, 2020. Use your confirmation number to determine whether you have been selected on Entrant Status Check, available at dvselectee.state.gov.

5

HOW TO RESPOND.
If selected, follow the instructions on Entrant Status Check. dvselectee.state.gov.

6

INTERVIEW PROCESS.
Selected individuals who respond to the instructions provided on Entrant Status Check will receive notification of their scheduled IV appointment through Entrant Status Check. The immigrant visa application fee is paid at the Embassy or Consulate at the time of the interview. This is the **ONLY** fee the U.S. government charges for the DV program.

TIPS:
Avoid Fraud & Scams: Some websites and emails try to mislead customers into thinking they are official U.S. government websites.
Do your own application: The online entry application is simple and free of charge.
Follow the rules: Read the application instructions carefully to avoid disqualification at dvlottery.state.gov.

travel.state.gov

Figure 9.37 The U.S. Department of State Diversity Visa Program.

9.3.2 Project Shield America Initiative

Project Shield America seeks to prevent foreign adversaries, terrorists, and criminal networks from obtaining and trafficking in WMDs (Figure 9.38).

The program seeks to thwart terrorist groups from obtaining sensitive information about American technologies, commodities, munitions, and firearms. Furthermore, Project Shield America traces financial transactions that violate U.S. sanctions or embargos. It also checks the propriety of exports to determine whether the goods shipped are legal and consistent with the laws of the United States. Most importantly, the program focuses on high-level technology that can be used against the United States in negative ways. The types of exported technology that would be subject to Project Shield America's scrutiny would encompass

- Modern manufacturing technology for the production of microelectronics, computers, digital electronic components, and signal processing systems
- Technology necessary for the development of aircraft, missile, and other tactical weapon delivery systems
- All types of advanced signal and weapons detection, tracking, and monitoring systems
- Technology and equipment used in the construction of nuclear weapons and materials
- Biological, chemical warfare agents and precursors, and associated manufacturing equipment.

Project Shield America tackles its job in three fundamental ways.

- *Inspection and interdiction:* Working at ports especially, both USCIS and CBP monitor potential harms.
- *Investigations and outreach:* USCIS conducts wide-ranging criminal investigations dealing with illegal munitions. In addition, the program educates exporters and importers on legal compliance.
- *International cooperation:* The agency helps support investigations by foreign law enforcement into illegal weapons and technology trafficking.



Figure 9.38 Project Shield America logo.

Homeland Security

In the area of prohibited goods, illegal trafficking in goods, or other prohibited items, ICE has issued a series of *red flags* that tip the practitioner into a more suspicious mindset of potential or actual criminal purposes. See the following list of common red flags:

RED FLAGS: INDICATIONS OF POTENTIAL ILLEGAL EXPORTS

ICE solicits the assistance of private industry to share information related to suspicious acquisitions of high technology and munitions or services relating to these items. The following are possible indicators of illegal exports or diversions.

- The customer is willing to pay cash for a high-value order rather than use a standard method of payment, which usually involves a letter of credit.
- The customer is willing to pay well in excess of market value for the commodities.
- The purchaser is reluctant to provide information on the end-use or end-user of the product.
- The end-use information provided is incompatible with the customary purpose for which the product is designed.
- The final consignee is a trading company, freight forwarder, export company or other entity with no apparent connection to the purchaser.
- The customer appears unfamiliar with the product, its application, support equipment or performance.
- The packaging requirements are inconsistent with the shipping mode or destination.
- The customer orders products or options that do not correspond with their line of business.
- The customer has little or no business background.
- Firms or individuals from foreign countries other than the country of the stated end-user place the order.
- The order is being shipped via circuitous or economically illogical routing.
- The customer declines the normal service, training, or installation contracts.
- The product is inappropriately or unprofessionally packaged (e.g., odd-sized/retaped boxes, hand lettering in lieu of printing, altered labels or labels that cover old ones).
- The size or weight of the package does not fit the product described.
- “Fragile” or other special markings on the package are inconsistent with the commodity described.⁵⁰

Internet Exercise: Read about legal cases and prosecutions of violators caught because of Project Shield America at <http://www.ice.gov/news/library/factsheets/counter-proliferations.htm>.

9.3.3 Fugitive Operations Program

On February 25, 2002, the National Fugitive Operations Program (NFOP) was officially established under the banner department of ICE. The primary mission of NFOP is to identify, locate, apprehend, process, and remove fugitive aliens from the United States, with the highest priority placed on those fugitives who have been convicted of crimes. Furthermore, NFOP’s goal is to eliminate the backlog of fugitives and ensure that the number of aliens deported equals the number of final orders of removal issued by the immigration courts in any given year.

The NFOP fugitive operations teams strategically deployed around the country work solely on those cases identified as fugitives and attempt to locate and apprehend those persons who will ultimately be removed from the United States. The NFOP publishes a “most wanted” list of criminals, terrorists, and other unsavory characters.

Internet Exercise: To regularly and currently keep up with the ICE list of foreign criminal aliens, visit <https://www.ice.gov/most-wanted#tab1>.

The NFOP training course is conducted at the ICE Academy located at the Federal Law Enforcement Training Center (FLETC). The training stresses utilization of the Internet, databases, and other sources of information to locate where a fugitive lives, visits, and works. NFOP teams are frequent participants in joint task forces at the state and local levels.

9.3.4 Cornerstone Initiative

Terrorist and other criminal organizations need cash and finance to support illegal operations. The Cornerstone Initiative detects and closes those means to exploit the financial sector. Some of the more common targets of enforcement are

- Bulk cash smuggling
- Alternative financing mechanisms used to launder illicit proceeds
- Money service businesses, financial institutions, and international trade and transportation sectors
- Common highly profitable cross-border crimes such as commercial fraud, intellectual property rights (IPR) violations, immigration violations, identity and benefits fraud, contraband and alien smuggling, and human trafficking
- Trade-based money laundering (TBML) using the international trade system to disguise illicit proceed by altering customs and banking paperwork

The Cornerstone team looks for patterns and select indicators of behavior in the transfer of money and funds.⁵¹ There are a host of red flags that indicate the money trail is out of mainstream financial practice. Within the Cornerstone Initiative rests the National Bulk Cash Smuggling Center, which works with diverse law enforcement agencies nationally and internationally in seeking to end the smuggle of large cash sums. Such sums are usually associated with drugs and other nefarious acts.

During the Covid-19 pandemic, ICE's Cornerstone program has identified and highlighted a rather large group of foreign criminals engaging in fraudulent practices and criminal activities. It just reported the examples at Figure 9.39.⁵²

Internet Exercise: To learn about the complexities of law enforcement's efforts to combat cash smuggling visit the center's FAQ at <http://www.ice.gov/bulk-cash-smuggling-center/faq/>.

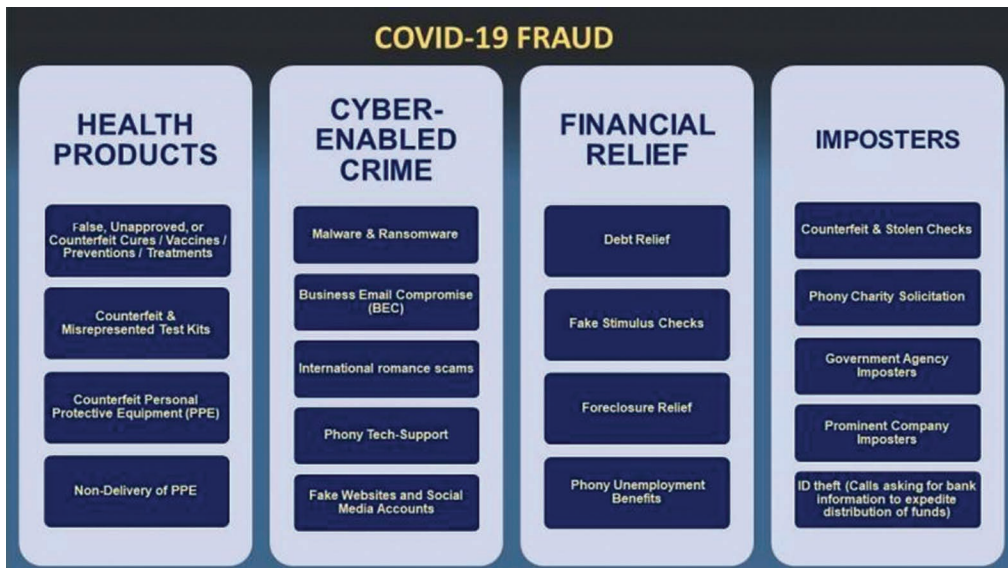


Figure 9.39 Various forms of fraudulent COVID fraud and crimes.

9.3.5 Cyber Crimes Center

Created in 1997, the Cyber Crimes Center, known as C3, brings a full range of ICE computer and forensic assets together in a single location to combat such Internet-related crimes as possession, manufacture, and distribution of child pornography; money laundering and illegal cyber banking; arms trafficking and illegal export of strategic/controlled commodities; drug trafficking; trafficking in stolen art and antiquities; and intellectual property rights violations. Cybercrimes units are not exclusively the province of CBP but exist side by side in many federal and state agencies, including the FBI and large metropolitan police departments.⁵³

There are serious critics of the type of oversight and intervention evident in forensic computing and software. Civil libertarians constantly wail about privacy considerations, and policymakers need always keep their practices in check in light of these considerations.⁵⁴

Much of what the Cyber Crimes Center undertakes relates to child pornography. The scourge of predators and their tie to cyber pornography are amply documented. ICE's child exploitation unit, iGuardians, and now Cyber Predators, tackles this difficult and emotionally wrenching job (Figure 9.40).

The Virtual Global Taskforce (VGT) is made up of law enforcement agencies from around the world working together to fight child abuse online. VGT aims to build an effective, international partnership of law enforcement agencies that helps to protect children from online child abuse. VGT (Figure 9.41) strives to make the Internet a safer place; to identify, locate, and help children at risk; and to hold perpetrators accountable.

VGT comprises the Australian High Tech Crime Centre, the Child Exploitation and Online Protection Centre in the United Kingdom, the Royal Canadian Mounted Police, the U.S. DHS, the Italian Postal and Communication Police Service, and Interpol. ICE's Operation Predator program, in collaboration with national and international partners, targets the worst of the worst in the dark world of child victimization. In addition, ICE maintains a National Child Victim Identification System.

Since 9/11, the USCIS, through its enforcement unit, the ICE division, has used these pertinent skills in the hunt for the terrorist as well. The mission of the Cyber Crimes Center is to investigate domestic and international criminal activities occurring on or facilitated by the Internet. The Cyber Crimes Center is blessed with a state-of-the-art center that offers cyber-crime training to federal, state, local, and international law enforcement agencies.

Terrorists use the Internet and find the means and methods to conduct business, transfer funds, share information, and issue instructions. ICE distinguishes itself in the area of illegal arms and money laundering. ICE's Arms and Strategic Technology division looks to prevent the proliferation of weapons, as well as the movement of terrorists and other criminals from entering the United States.

The Cyber Crimes Center has an additional competence regarding documents and related fraud. If 9/11 made plain any conclusion, it was the ease with which terrorists could fabricate documents to gain access. The threat posed by document fraud is evidenced by the ease with which seven of the 9/11 hijackers obtained identity documents in the State of Virginia.

Passports are a particular problem for USCIS since the range and design will depend on the country of issue. Figure 9.42 shows an example of a counterfeit passport card used by a terrorist who was caught before his attempted act of terror at the Los Angeles airport in 1999. He is presently serving a 22-year term in a federal penitentiary.

Documents give telltale signs of fraud, and Customs and Immigration personnel have been trained to detect it. The more common fraud indicators are

- Physically altered passports
- Passports with serial numbers that are watch listed as lost or stolen
- Handwritten documents that are easily forged or altered



 **U.S. Immigration
and Customs
Enforcement**

MISSION

Project iGuardian is focused on keeping children and teens safe from online predators through education and awareness. The project is an outreach effort to share information about the dangers of online environments, how to stay safe online and how to report abuse and suspicious activity. In addition, the iGuardians team is here to help kids stay safe online by providing safety tips, a number to call and a website with links to more information and resources.

THINK BEFORE YOU CLICK
To report abuse call **1-866-DHS-2-ICE**
www.ice.gov/iguardsian



Figure 9.40 Project iGuardian helps kids, teens, and parents to be smart about online safety and stay safe from online sexual predators. (From U.S. Immigration and Customs Enforcement, www.ice.gov/guardian.)



Making the internet a safer place > www.virtualglobaltaskforce.com

Figure 9.41 VGT is a group of law enforcement agencies from around the world working together to fight child pornography online. (From Virtual Global Taskforce, <http://virtualglobaltaskforce.com/>.)



Figure 9.42 Counterfeit passport.

- Multiple passports used by the same person with variations in the spelling/structure of the name and date of birth
- Ambiguous or contradictory information submitted to consular or border control officials
- Absence of supporting documents to corroborate passport information

- Passports with glued-in photographs
- Large gaps in travel history as reflected in stamps and visas

Internet Exercise: The U.S. Department of State has authored a quick course in passport fraud available at the Department of State's Archived website at <https://2009-2017.state.gov/m/ds/investigat/cl0714.htm>.

9.3.6 US-VISIT Program/Office of Biometric Identity Management

DHS's US-VISIT program, now renamed the Office of Biometric Identity Management (OBIM), provides visa-issuing posts and ports of entry with biometric technology that enables the U.S. government to establish and verify the identities of those who visit the United States (Figure 9.43).

Internet Exercise: Find out about the many services OBIM provides by visiting <http://www.dhs.gov/obim-biometric-identification-services>.

This process begins overseas at a U.S. visa-issuing post, where a traveler's biometrics—digital fingerprints and a photograph—are collected and checked. Upon arrival in the United States, these same biometrics verify the identity of that person at the port of entry.

The guiding principles of OBIM are to

- Enhance the security of our citizens and visitors.
- Facilitate legitimate travel and trade.
- Ensure the integrity of the immigration system.
- Protect the privacy of our visitors.



Figure 9.43 Many federal, state, and local agencies use OBIM services. (From Homeland Security. Office of Biometric Identity Management, <https://www.dhs.gov/obim>.)

Homeland Security

Even though OBIM is an additional layer of security, most travelers will not notice the difference. At an airport or seaport, travel documents, such as a passport and a visa, will be reviewed and a U.S. CBP officer will ask specific questions regarding the visitor's stay in the United States.

Visitors traveling on visas will have two fingerprints scanned by an inkless device and a digital photograph taken. Data and information are then used to assist the border inspector in determining whether to admit the traveler. All data obtained from the visitor are securely stored as part of the visitor's travel record. This information is made available only to authorized officials and selected law enforcement agencies on a need-to-know basis in their efforts to help protect the country against those who intend to harm American citizens or visitors to the United States.

9.4 Conclusion

Protection of the border rightfully consumes the energy of the homeland community. The idea of border extends far beyond any notions of continental geography but includes the diverse ways in which visitors to the United States can find entry. Soon after 9/11, DHS recognized the need to subsume the functions of Border with those of Customs—erecting a new department, CBP. The work of CBP is extensive and includes encounters with millions of passengers and pedestrians, thousands of truck, rail, and sea containers and air travelers, shipments, and the computation of tariffs, duties, and other fees. More than a million illegal aliens have been apprehended since 2004. CBP has also erected targeted operations such as SBI, which increases manpower and resources across the entire national border. SBI upgrades all facets of border hardware and infrastructure, employs new technology to discover breaches in the border, and erects and maintains natural and artificial barrier systems to stem illegal entry. The rise in Border Patrol agents—some 50,000 additional needed in the next decade—proves the seriousness of the task.

CBP continually adds sophisticated equipment and technology to carry out its mission. The use of drones and other unmanned air devices is now part and parcel of the delivery system. CBP now has an A&M division that zeroes in on breach locations or unsafe entry points. Seven hundred pilots now man 300 aircraft in this challenge.

CBP assumes an integral role in the world of trade and commerce. With its cargo responsibilities, CBP scans and screens incoming cargo throughout the nation and even in foreign ports before its departure to the United States. In its SFI, radiation scanners inspect large-scale shipping holds before ever leaving worldwide ports. Usually at megaports such as England's Southampton or Singapore, the SFI not only scans vessels but registers and tracks them over the life of their journey. In the area of cargo containers, the CSI inspects incoming goods by both radiation and x-ray. The CSI is operational in foreign ports as well, covering 80% of the world's cargo destined to the United States. CBP partners with private companies in shipping and cargo through its C-TPAT program. C-TPAT promotes efficiency in cargo processes and serves as a liaison for business and industry security practices and the requirements of CBP. Electronic modernization of cargo manifests and other practices are made possible by the protocols of the ACE program.

In the area of immigration and citizenship, the DHS department of USCIS, once referred to as the INS, administers the status of immigrants, their claims, and adjudication processes, as well as promulgates protocols on naturalization, asylum, and refugee petitions and the granting or denial of visas. The Project Shield America initiative is a USCIS function that tracks illegal financial transactions, illegal munitions, and trafficking in contraband and WMDs. USCIS runs NFOP, which targets a most wanted list of illegal aliens and criminals. The USCIS administers a host of other programs relating to cybercrime and fraud, financial support for terrorists transfers, and passport forgery.

Keywords

Air and Marine; Amnesty; Automated Commercial Environment; Automated Commercial System; Biometrics; Border Patrol; Citizenship and Immigration Services; Common Operating Procedure; Container Security Initiative; Contraband; Cornerstone Initiative; Customs; Customs and Border Protection; Customs-Trade Partnership against Terrorism; Cyber Crimes Center; Fugitive Operations Team; Global Trade Exchange; The Great Wave; Illegal Immigration; Immigrant; Immigration and Naturalization Service; Immigration Reform; Marine Interdict Officer; Megaport; National Fugitive Operations Program; National Targeting Center; Natural Barriers; Naturalization; Partner Ports; Ports of Entry; Project Shield America; Radiation Portal Monitor; Refugees; Secure Border Initiative; Secure Data Portal Account; Secure Freight Initiative; SFI Scan; Transient Workers; US-VISIT; Visa

Discussion Questions

1. Given the resource and expenditure investment in border security, is it fair to expect safe and secure borders? Is there a correlation between the dollars invested and success at the border?
2. Evaluate how the merger of Border, Customs, and Immigration into DHS has affected the operational outlook of these former agencies. Has it been a healthy merger?
3. Discuss how armed law enforcement aids plane and travel security. Highlight specific programs.
4. Critics of the border fencing hold that it cannot work. Why not?
5. Lay out three perennial problems in the protection of U.S. borders.
6. In what ways does CBP aid or interfere with commerce?

Practical Exercises

1. Debate the public sentiment concerning illegal aliens?
2. Visit usajobs.gov. Create a job database of present opportunities for Border, Customs, and Immigration officers. Provide examples of each career opportunity.
3. Prepare a form file for the ACE program.
4. Customs deals with trade in diverse ways. Give four examples of how technology aids or even eliminates manpower in the moves of trade.
5. Take the naturalization test for citizenship administered by Immigration and Citizenship. Evaluate the level of ease or difficulty.

Notes

- 1 L. C. Frederking, A comparative study of framing immigration policy after 11 September 2001, *Policy Studies* 33, (2012): 283; M. Haberfield, C. A. Lieberman, Foreign threats to national security and an alternative model to local enforcement of US immigration laws, *Police Practice & Research* 13, (2012): 155.

Homeland Security

- 2 US Customs and Border Protection, Snapshot: A summary of CBP fact and figures, January 2020, <https://www.cbp.gov/sites/default/files/assets/documents/2020-Feb/CBP-Snapshot-Feb-2020.pdf> (accessed August 19, 2020).
- 3 US Coast Guard, Compass, Week in the life of the Coast Guard, August 8, 2012, <https://coastguard.dodlive.mil/tag/u-s-border-patrol/> (accessed August 19, 2020).
- 4 US Customs and Border Protection, CBP Organization Chart, <https://www.cbp.gov/document/publications/cbp-organization-chart> (accessed August 19, 2020).
- 5 US Customs and Border Protection, CBP Enforcement Statistics Fiscal Year 2020, <https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics> (accessed August 19, 2020); For previous years, see: Source: CBP, Performance and Accountability Report: Fiscal Year 2014 (2014), 8, https://www.cbp.gov/sites/default/files/documents/CBP_DHS_2014%20PAR_508C.PDF (accessed August 19, 2020).
- 6 And this is not a uniquely American experience either. See R. Nicholson, Swedish open immigration policies: Correlation with terrorism, *The Homeland Security Review*, 4 (2010): 193.
- 7 See: US CBP, From the Air and Sea Webpage, <https://www.cbp.gov/border-security/air-sea> (accessed August 19, 2020).
- 8 W. Ewing, Looking for a quick fix: The rise and fall of the Secure Border Initiative's high-tech solution to unauthorized immigration, *Immigration Policy Center: Just the Facts*, April 15, 2010, <https://www.americanimmigrationcouncil.org/research/rise-and-fall-secure-border-initiative%E2%80%99s-high-tech-solution-unauthorized-immigration> (accessed August 19, 2020).
- 9 Ibid, 1.
- 10 J. S. Passel and D. Cohn, Mexicans decline to less than half the US unauthorized immigrant population for the first time, FACTANK, June 12, 2019, Pew Research Center, https://www.pewresearch.org/fact-tank/2019/06/12/us-unauthorized-immigrant-population-2017/ft_19-06-12_unauthorizedimmigration_unauthorized-immigrants-quarter-us-foreign-born-population-2/ (accessed August 19, 2020); See also A. Gonzalez-Barrera, More Mexicans leaving than coming to the U.S., *Pew Research Center: Hispanic Trends*, November 19, 2015, <http://www.pewhispanic.org/2015/11/19/more-mexicans-leaving-than-coming-to-the-u-s/> (accessed August 19, 2020).
- 11 C. Bolkcom, *Homeland Security: Unmanned Aerial Vehicles and Border Surveillance* (Washington, DC: Library of Congress, 2005), <http://www.fas.org/sgp/crs/homsec/RS21698.pdf> (accessed August 19, 2020); *Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination Is Needed for the Northern Border* (2010); *Border Security: Additional Actions Needed to Better Ensure a Coordinated Federal Response to Illegal Activity on Federal Lands* (2010); *Moving Illegal Proceeds: Challenges Exist in the Federal Government's Effort to Stem Cross-Border Currency Smuggling* (2010); *Border Security: Preliminary Observations on the Status of Key Southwest Border Technology Programs* (2011); *Moving Illegal Proceeds: Opportunities Exist for Strengthening the Federal Government's Efforts to Stem Cross-Border Currency Smuggling* (2011); *Border Security: Preliminary Observations on Border Control Measures for the Southwest Border* (2011). See also: US Dept of Homeland Security, Border Security Overview Web page, <https://www.dhs.gov/border-security-overview> (accessed August 19, 2020).
- 12 See: US Government Accountability Office, Letter of September 5, 2019 regard Department of Defense-Availability of Appropriation for Border Fence Construction, <https://www.gao.gov/assets/710/701176.pdf> (accessed August 19, 2020).
- 13 U.S. Government Accountability Office, *Border Security: DHS Progress and Challenges in Securing the U.S. Southwest and Northern Borders* (Washington, DC: U.S. Government Printing Office, 2011).
- 14 See: U.S. Government Accountability Office, Southwest Border Security: Additional Actions Needed to Better Assess Fencing's Contributions to Operations and Provide Guidance for Identifying Capability Gaps GAO-17-331, February 16, 2017, <https://www.gao.gov/products/GAO-17-331> (accessed August 18, 2020); See also: U.S. Government Accountability Office, Border Security: Assessment of the Department of Homeland Security's Border Security Improvement Plan GAO-19-538R, July 16, 2019, <https://www.gao.gov/products/GAO-19-538R> (accessed August 18, 2020).
- 15 U.S. Department of Homeland Security, Fact Sheet: DHS Agreements with Guatemala, Honduras, and El Salvador, https://www.dhs.gov/sites/default/files/publications/19_1028_opa_factsheet-northern-central-america-agreements_v2.pdf (accessed August 18, 2020).
- 16 See: "How border apprehensions, ICE arrests and deportations have changed under Trump." By John Gramlich. Pew Research Center, Washington, D.C. (March 2, 2020), https://www.pewresearch.org/fact-tank/2020/03/02/how-border-apprehensions-ice-arrests-and-deportations-have-changed-under-trump/ft-20-02-24_trumpimmigrationenforcement_1 (accessed August 19, 2020).

- 17 H. Hogan, CBP's best- and newest-friends, *Homeland Security Today*, 17, July 2011.
- 18 See: Homeland Security Advisory Council, Final Emergency Interim Report: CBP Families and Children Care Panel, 17 (April 16, 2019), https://www.dhs.gov/sites/default/files/publications/19_0416_hsic-emergency-interim-report.pdf (accessed August 19, 2020).
- 19 T. Steinmetz, Mitigating the exploitation of U.S. borders by jihadists and criminal organizations, *Journal of Strategic Security*, 4 (2011): 35.
- 20 To see the laws that guide enforcement of human trafficking, visit: US Dept of Homeland Security, Human Trafficking Law & Regulations Webpage, <https://www.dhs.gov/human-trafficking-laws-regulations> (accessed August 19, 2020).
- 21 US Dept of Homeland Security, Office of Intelligence and Analysis, Mexico: Cross-Border Gangs and their Mexican Drug Cartel Affiliations, <https://info.publicintelligence.net/DHS-MexicoCrossBorderGangs.pdf> (accessed August 19, 2020).
- 22 See: US Government Accountability Office, U.S. Assistance to Mexico GAO-19-647, <https://www.gao.gov/assets/710/701281.pdf> (accessed August 19, 2020).
- 23 See Presidential Proclamation Addressing Mass Migration Through the Southern Border of the United States, November 9, 2018, <https://www.whitehouse.gov/presidential-actions/presidential-proclamation-addressing-mass-migration-southern-border-united-states/> (accessed August 19, 2020).
- 24 US CBP, Air and Marine Operations Missions Webpage, <https://www.cbp.gov/border-security/air-sea/missions> (accessed August 19, 2020).
- 25 US CBP, Air and Marine Operations Fact Sheet, https://www.cbp.gov/sites/default/files/assets/documents/2020-Apr/FS_2020_AMO_Fact%20Sheet_FINAL_508__0.pdf (accessed August 19, 2020).
- 26 US CBP, Coastal Enforcement Class 10-foot Intrepid Fact Sheet, https://www.cbp.gov/sites/default/files/documents/FS_2015_30%20Ft%20Intrepid_FINAL.pdf (accessed August 19, 2020).
- 27 See: US Dept of Homeland Security, Unmanned Aerial Systems webpage, <https://www.dhs.gov/science-and-technology/unmanned-aerial-systems> (accessed August 19, 2020).
- 28 US Dept of Homeland Security, Emerging Risk to Infrastructure from Unmanned Aerial Vehicles (May 2016), <https://info.publicintelligence.net/DHS-InfrastructureThreatsUAVs.pdf> (accessed August 19, 2020).
- 29 CBP, *CBP Trade Strategy 2009–2013* (Washington, DC: CBP, 2009), 24. See also: US CBP, *Strategy 2020–2025*, (2020) <https://www.cbp.gov/sites/default/files/assets/documents/2019-Jun/CBP-2020-2025-Strategy-Plan-Documents-FINAL-508-compressed.pdf> (accessed August 19, 2020).
- 30 US CBP, *Strategy 2020–2025*, 5 (2020) <https://www.cbp.gov/sites/default/files/assets/documents/2019-Jun/CBP-2020-2025-Strategy-Plan-Documents-FINAL-508-compressed.pdf> (accessed August 19, 2020).
- 31 US CBP, *CBP Trade Strategy 2020* Publication Number 0814-1018, <https://www.cbp.gov/sites/default/files/assets/documents/2018-Oct/Trade-Strategy-2020.pdf> (accessed August 19, 2020).
- 32 For the text of the Act, see: <https://uscode.house.gov/view.xhtml?path=/prelim@title6/chapter3&edition=prelim> (accessed August 19, 2020).
- 33 US CBP, *Strategy 2020–2025*, 13 (2020), <https://www.cbp.gov/sites/default/files/assets/documents/2019-Jun/CBP-2020-2025-Strategy-Plan-Documents-FINAL-508-compressed.pdf> (accessed August 19, 2020).
- 34 US CBP, Container Security Initiative Office of Field Operations (2/2014), <https://www.cbp.gov/sites/default/files/documents/CSI%20Ports%20Map%201%20page%20062614.pdf> (accessed August 19, 2020).
- 35 CBP, CSI: Container Security Initiative, <http://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief> (accessed August 19, 2020).
- 36 See: US CBP, Getting Started with SBP Automated Systems Webpage, <https://www.cbp.gov/trade/automated/getting-started> (accessed August 19, 2020).
- 37 The White House Archive, Streamlining legal immigration, <https://obamawhitehouse.archives.gov/issues/immigration/streamlining-immigration> (accessed August 19, 2020); The White House Archive, Continuing to strengthen border security, <https://obamawhitehouse.archives.gov/issues/immigration/border-security> (accessed August 19, 2020); The White House Archives, Earned citizenship, <https://obamawhitehouse.archives.gov/issues/immigration/earned-citizenship> (accessed August 19, 2020).

Homeland Security

- 38 American Immigration Council, “Fact Sheet – Sanctuary Policies: An Overview,” October 21, 2020 <https://www.americanimmigrationcouncil.org/research/sanctuary-policies-overview>.
- 39 Kagan, Michael, “What We Talk About When We Talk About Sanctuary Cities” (2018). *Scholarly Works*. 1140. Vol. 52:391, p. 396.
- 40 US Citizenship and Immigration Services, Archive, Consideration of Deferred Action for Childhood Arrivals (DACA), <https://www.uscis.gov/archive/consideration-deferred-action-childhood-arrivals-daca> (accessed August 19, 2020).
- 41 See: M. W. McConnell, Michael McConnell on Executive Orders, DACA, and the Constitution, September 6, 2017, Stanford Law School Blogs, <https://law.stanford.edu/2017/09/06/michael-mcconnell-on-executive-orders-daca-and-the-constitution/> (accessed August 19, 2020); See also: US Dept of Homeland Security, Deferred Action for Childhood Arrivals (DACA) Webpage, <https://www.dhs.gov/deferred-action-childhood-arrivals-daca> (accessed August 19, 2020).
- 42 White House Fact Sheet, President Donald J. Trump Restores Responsibility and the Rule of Law to Immigration, September 5, 2017, <https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-restores-responsibility-rule-law-immigration/> (accessed August 19, 2020).
- 43 US Dept of Homeland Security v. Regents of Univ of California, et al, Slip Opinion, 5, October term, 2019, No 18-587 (US Supreme Court, 2018), https://www.supremecourt.gov/opinions/19pdf/18-587_5ifl.pdf (accessed August 19, 2020).
- 44 See: US Citizenship and Immigration Services, Green Card Through the Diversity Immigrant Visa Program Webpage, <https://www.uscis.gov/green-card/green-card-eligibility/green-card-through-diversity-immigrant-visa-program> (accessed August 19, 2020).
- 45 US Dept of State, 2021 Diversity Visa Program Instructions, https://travel.state.gov/content/dam/visas/Diversity-Visa/DV-Resources/Diversity%20Visa%20Infographic_10-2019.pdf (accessed August 19, 2020).
- 46 See: US Dept of Homeland Security, We Need to End Unchecked Chain Migration and Eliminate the Reckless Visa Lottery to Secure the Nation and Protect the American Worker, Press Release February 15, 2018, <https://www.dhs.gov/news/2018/02/15/we-need-end-unchecked-chain-migration-and-eliminate-reckless-visa-lottery-secure#content> (accessed August 19, 2020).
- 47 See: White House Fact Sheet, Facing the Facts About Our Broken Immigration System, January 30, 2018, <https://www.whitehouse.gov/briefings-statements/facing-facts-broken-immigration-system/> (accessed August 19, 2020).
- 48 See: Federation for American Immigration Reform, Understanding Chain Migration, <https://www.fairus.org/issue/legal-immigration/chain-migration> (accessed August 19, 2020).
- 49 See: The White House, It’s Time to End Chain Migration, December 15, 2017, <https://www.whitehouse.gov/articles/time-end-chain-migration/> (accessed August 19, 2020).
- 50 US Immigration and Customs Enforcement, Project Shield America Webpage, <https://www.ice.gov/project-shield-america> (accessed August 19, 2020).
- 51 Homeland Security Investigations: Trade Transparency Unit, *The Cornerstone Report*, Winter 2011.
- 52 See: US Immigration and Customs Enforcement, Cornerstone Webpage, <https://www.ice.gov/cornerstone> (accessed August 19, 2020).
- 53 A. P. Gerglas, The New York FBI and the cyberthreat, *Homeland Security Today* (July 2011): 6; See also J. R. Wilson, IT & cyber security, *Year in Homeland Security* (2010/2011): 83.
- 54 M. McCarter, ID Management, *Homeland Security Today* (August 2011): 48.

10

Transportation Security

OBJECTIVES

1. To describe the mission and scope of operation of the Transportation Security Administration (TSA)
2. To explain the programs and policies created by TSA to ensure secure air transportation in the United States
3. To outline the technological advances in transportation security in use at airport screening points
4. To describe the mission and scope of operation of the U.S. Coast Guard
5. To explain the programs and policies created by the U.S. Coast Guard to ensure secure maritime transportation in the United States
6. To outline the technological advances in security in use at maritime and cargo screening points
7. To explain the programs and policies in place to ensure secure passenger rail transportation in the United States
8. To explain the programs and policies in place to ensure secure cargo rail transportation in the United States

10.1 Introduction

In the broadest context, transportation security encompasses air, rail, bus, shipping and ports, and mass transit safety. Most of these centers of movement can properly be characterized as critical infrastructure. Many agencies of government deal with transportation safety and security questions. The Department of Homeland Security (DHS) and Federal Aviation Administration (FAA) first come to mind since each regulates and promulgates administrative practices regarding these industries. The Department of Commerce involves itself in a host of travel questions, as does the Federal Highway Administration. Because of the multiagency involvement in the world of travel and transportation, it would be impossible to cover each and every aspect of the homeland question relative to the diversity of government agencies and missions. What we will try to do is highlight the most relevant for homeland security purposes, starting with TSA.

10.2 Transportation Security Administration

Of any portion of the homeland security enterprise, the one that touches the general public the most is the work of TSA. Most American citizens come face-to-face with TSA—the visible arm of airport safety in our terminals. Passenger and baggage screening are the prime tasks of TSA. Despite these responsibilities, TSA engages in a broad range of other activities. TSA is a component of DHS and not only is responsible for the security of the country's airline transportation systems, but also, with state, local, and regional partners, oversees security for the highways, railroads, buses, mass transit systems, ports, and the 450 U.S. airports. TSA employs approximately 60,000 people. TSA is a large bureaucracy that has yet to fully find its way, nor has it successfully captured significant public support in how it carries out its mission. In many ways, TSA antagonizes far too many constituencies, and in other ways, it really has a thankless and difficult job. Controversial practices include enhanced physical pat-down searches of young children and the elderly as well as scanners that provide near-naked pictures of passengers.¹ Scandals include naked body imagery shared on the Internet, undetected contraband making it through screenings at various airports, and TSA agents indicted for corruption and drug trafficking. TSA has tried to counter the bad press with an aggressive use of social media.² It is well aware of how public aggravation at the screening process, increasing public distrust, and the agency's high attrition rate undercut its efforts to become a professional body.³ And the morale problem has increased during the COVID-19 pandemic with scores of TSA employee infections and even deaths amongst its rank and file.⁴

In 2010, TSA began a program with Global Corporate College—provided through regional community colleges around the country—to further educate and train TSA employees. In addition, it has recently engaged in a series of public relations campaigns to bolster its image. See Figure 10.1 for an example from a public relations campaign.⁵

The agency designates a public affairs officer line in its organizational structure (Figure 10.2).⁶

TSA recently adopted a series of core values that stress the professionalism and integrity it aspires to. The agency indicates the need for a positive “culture” to carry out its stated mission. See Figure 10.3.⁷

The bulk of the TSA's activities relate to airline safety. Indeed, if the terrorist attacks of 9/11 had occurred on a boat, the likely location for our front line of defense would have been in the harbor. Location has much to do with policy and practice. Then again, the nature of the 9/11

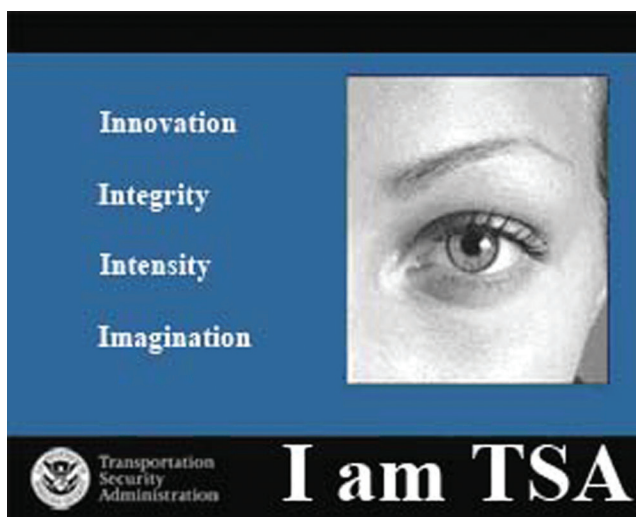


Figure 10.1 TSA public relations campaign.

10.2 Transportation Security Administration

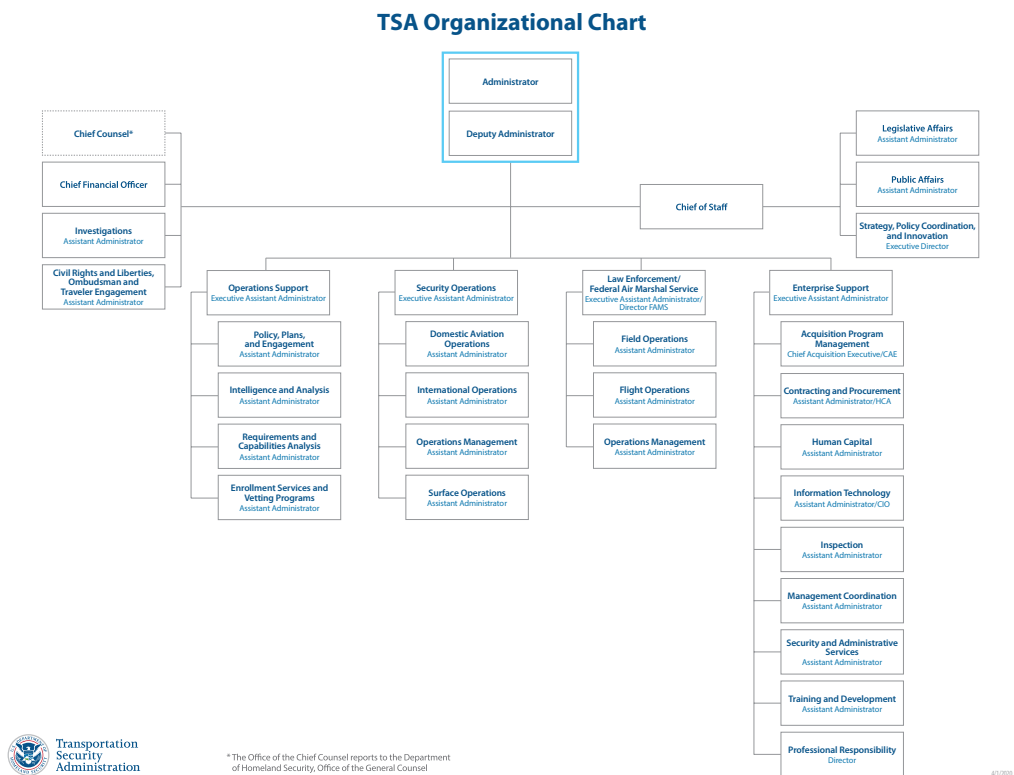


Figure 10.2 TSA organization chart.



Mission

Protect the nation's transportation systems to ensure freedom of movement for people and commerce.

Vision

An agile security agency, embodied by a professional workforce, that engages its partners and the American people to outmatch a dynamic threat.

Core Values

Integrity. Respect. Commitment.

Workforce Expectations

Hard work. Professionalism. Integrity.

Figure 10.3 TSA's stated mission and vision.

Homeland Security

attacks also prompted this emphasis. Perhaps not ideal, airport safety screening surely adds a layer of safety to the culture (Figure 10.4).⁸

And the pandemic has accelerated the demands and prompted even more requirements for travel.⁹ See the recent guidelines at Pittsburgh International Airport in Figure 10.5.



Figure 10.4 TSA officer at a security checkpoint.

- **Facial Coverings** – All employees, passengers and visitors are required (per CDC age and medical condition guidelines) to wear face coverings on *all public airport property* effective Monday, May 18.
- **Enhanced Cleaning and Disinfecting** –
 - Frequent deep cleaning practices continue in all public spaces and restrooms, and additional hand sanitizing stations have been added.
 - PIT is pioneering the use of UV light in airport public areas such as floors, moving walkways, elevators and escalator rails to reduce contaminants and provide another layer of sanitation.
- **Protective Shields** – Shields and barriers are being installed in high -traffic areas, including public counters, checkpoints and baggage claim.
- **Social Distancing** – Signage and floor markings throughout the terminal will give guidance on six -foot distancing in common areas.
- **Reconfigured Seating** – Furniture in gate areas, food court and baggage claim are being removed or repositioned to allow for social distancing.
- **Touchless Transactions** – PIT is evaluating touchless technology for concessions and parking transactions.

Figure 10.5 TSA safety guidelines as posted at Pittsburgh International Airport.

10.2 Transportation Security Administration

TSA's primary mission is transportation—all forms and all locales. It is a gargantuan responsibility. In 2014, TSA dealt with a staggering array of travelers, personnel, and issues. Consider the scope of the jurisdiction.

Aviation Security

- Responsible for the security of nearly 440 federalized airports
- Approximately 50,000 transportation security officers keep people secure
- More than 600 aviation transportation security inspectors ensure regulatory compliance
- Nearly 50% of TSA officers have 5 years or more experience as counterterrorism professionals
- Nearly 20% of TSA employees are veterans or still proudly serving
- TSA screens more than two million passengers daily and over 750 million every year
- TSA screens 1.4 million checked items for explosives and other dangerous items daily
- TSA screens 5.5 million carry-on items for explosives and other prohibited items every day
- Responsible for the security of over 23,000 domestic flights per day
- Responsible for the security of nearly 2,600 outbound international flights per day

Checkpoint Security and Risk-Based Security

- There are nearly 950 advanced imaging technology machines with privacy-protecting software at airports nationwide
- In 2019, officers detected approximately 4,432 firearms at airport checkpoints, averaging 12 firearms per day
- TSA conducts over 29,000 assessments a year to improve hands-on training with transportation security officers
- TSA risk-based security is based on the understanding that the vast majority of people traveling pose little to no threat to aviation and applies an intelligence-driven approach focusing on higher risk and unknown passengers. Through risk-based security:
 - There are over 400 TSA Pre® application centers open nationwide
 - TSA Pre® is operating at more than 200 airports
 - More than eight million passengers each week experience expedited screening

Inbound International Aviation

- TSA inspects approximately 280 last point-of-departure airports (those with direct flights into the United States)
- There are 109 countries with at least one last point-of-departure airport
- Responsible for securing nearly 700 foreign repair stations
- Approximately ten billion pounds of cargo is transported on commercial aircraft annually from foreign airports
- There are 40 recognized countries in the national cargo screening program

Law Enforcement

- Federal air marshals fly millions of miles each year supporting aviation security
- There are more than 1,000 TSA canine teams deployed nationwide tasked with screening passengers and cargo, and supporting other security missions

Homeland Security

- In 2019, more than 300,000 hours of canine explosives detection screening throughout the nation's transportation system
- Thousands of federal flight deck officers participate voluntarily to ensure the traveling public security
- Provide assistance to hundreds of crew member self-defense trainings yearly

Multi-modal Security Efforts

- TSA secures the U.S. transportation network which connects cities, manufacturers, and retailers through:
 - More than four million miles of roadways
 - Nearly 140,000 miles of railroad track
 - Approximately 612,000 bridges and more than 470 tunnels
 - Approximately 360 maritime ports, over 3,700 marine terminals and approximately 12,000 miles of coastline
 - Approximately 2.75 million miles of pipeline
 - Approximately 250 surface transportation security inspectors ensure the security of the surface transportation arena
 - More than 8,000 surface regulatory inspections are conducted annually in support of risk-based security
 - Nearly 30 million daily trips are taken on public transportation¹⁰

From airports to bus stations, rail terminals to pipelines, TSA is entrusted with extraordinary responsibilities. In each of these sectors, TSA must be mindful of the

- Completion of industry threat, vulnerability, and consequence assessment
- Development of baseline security standards
- Assessment of operator security status versus existing standards
- Development of plan to close gaps in security standards
- Enhancement of systems of security

TSA has generally accomplished its mission although there is always room for improvement. In the area of gun and weaponry confiscations TSA has shown some improvement, see Figure 10.6.

TSA has shown little hesitation in expanding its reach into all forms of transportation.¹¹ For example, the creation and implementation of the Visible Intermodal Prevention and Response (VIPR) program—including teams of local and federal law enforcement officers, along with TSA specialists combing the subways, the ferries, and all forms of public transportation—signifies TSA's reach over the entire national transportation system (Figure 10.7).

However, the VIPR program has been heavily critiqued for its excessive cost and lack of benefit. VIPR budgets were significantly cut in the TSA budget for 2020 some have even claimed the program began its terminal crawl in 2019.¹² Whatever system is reviewed, TSA's mission includes the development of various layers of security protection at the facilities it is entrusted with. By layers, we mean barriers or checkpoints for protection. The more checkpoints that exist, the greater the likelihood is that a threat is detected. In the aviation sector, the layers of security are both sophisticated and largely effective. TSA works to identify questionable passengers long before the security checkpoint, including intelligence analysis, watch lists and passenger manifests, random canine searches, and insertion of federal air marshals, flight deck officers, and crew. TSA charts these layers in Figure 10.8.

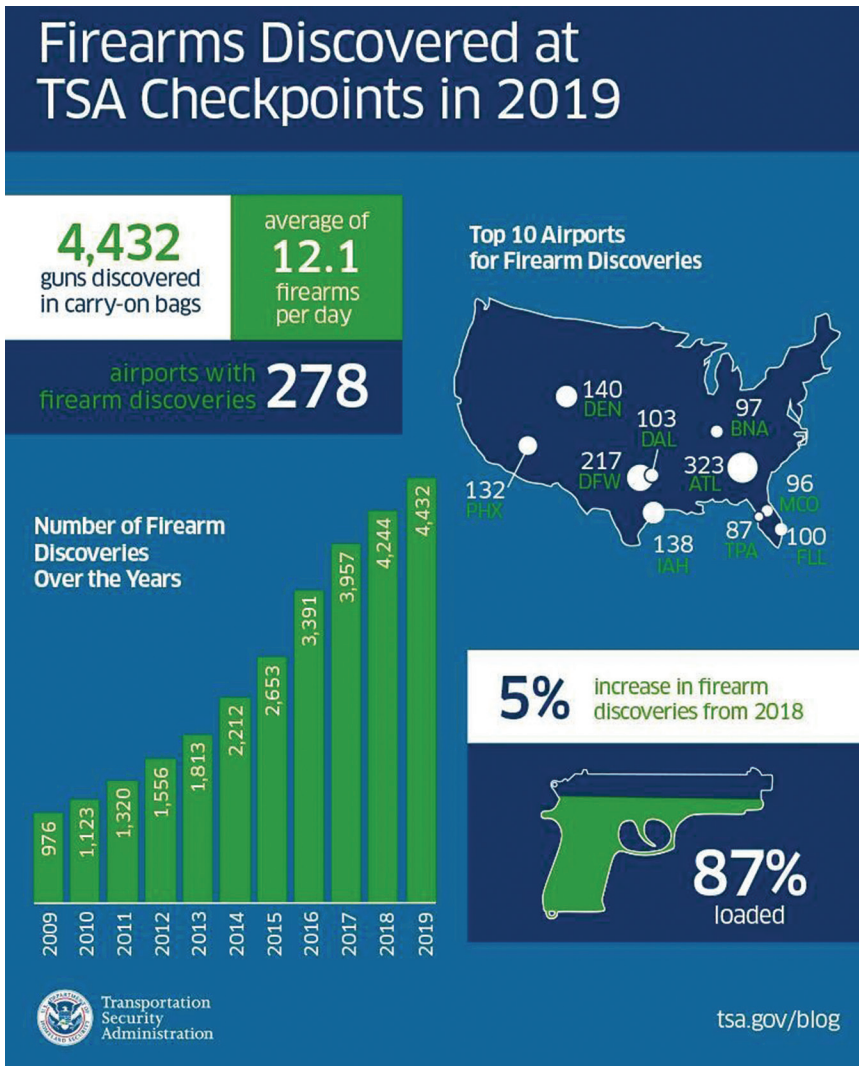


Figure 10.6 Statistics on firearms discovered at TSA checkpoints.

TSA also recognizes that it must rely on the public for constant vigilance and assistance in carrying out its mission. Its “If You See Something, Say Something” campaign encourages an active public partnership. See Figure 10.9.¹³

Internet Exercise: Find out about all the parameters of the “See Something, Say Something” program at <http://www.dhs.gov/see-something-say-something/about-campaign>.

At any given point along this detection continuum, the terrorist is vulnerable. Whether at the airport screening machine or vetted by random checks, in order to succeed, the terrorist will have to pass through a multitiered checkpoint system. The sheer volume of detection points reduces the chance for terrorist activity. See Figure 10.10.

Aside from staffing airport screening lines, TSA involves itself in a diversity of programs (Figure 10.11).



Figure 10.7 A VIPR team at Union Station in Washington, DC.

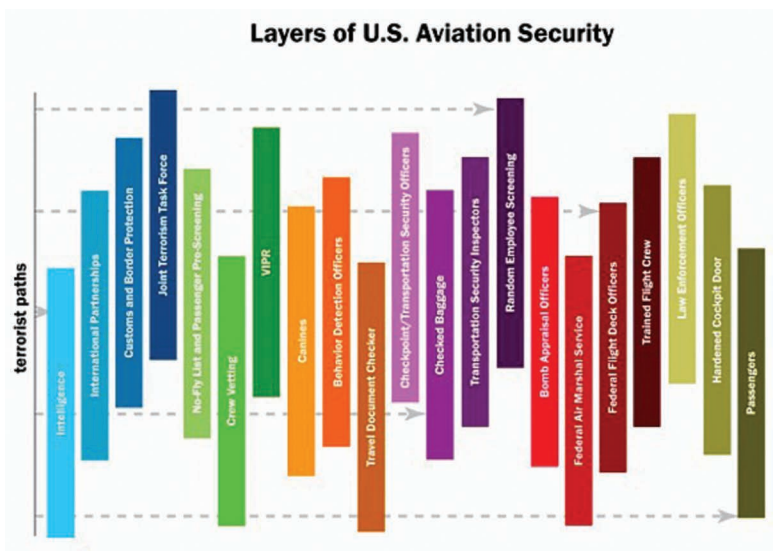


Figure 10.8 Layers of U.S. aviation security. (Source: DHS. Aviation security, <https://www.dhs.gov/aviation-security>.)

10.2.1 TSA and the Privatized Airport

While TSA has, on the whole, done a laudable job in carrying out its many responsibilities, it often suffers from a tin ear when complaints are filed or when becoming so big it lacks the flexibility to serve both the airport and its customers. TSA can be a lumbering giant and its capacity to adapt to a more consumer-based mentality, where travelers are customers, often seems a pipe-dream. And it is no secret that both airports and customers do not like the performance or the conduct of select TSA representatives. So regular has been this critique that Congress enacted an alternative option that allows airports to opt out of full TSA control and screening and the right to replace with private sector officers to conduct TSA services.

As previously commented upon, the TSA dissatisfaction rate and negative public sentiment have opened up a world of opportunity for the private security industry. With customer concern and its inherent results orientation, the private sector appears ready for a fully and unbridled



Figure 10.9 DHS and its partners raise public awareness of the indicators of terrorism and terrorism-related crime through the “If You See Something, Say Something” campaign. They engage and inform the public through television and radio public service announcements (PSAs), partner print materials, transit opportunities, billboards, and other media. An example of their print media is shown here. (From Department of Homeland Security. Transportation Security Administration. If you see something, say something, <https://www.tsa.gov/news/top-stories/2014/07/28/if-you-see-something-say-somethingTM>.)

return to its former home—the airport. Pre-9/11 reality is being replayed, albeit in a modified way as public outcries over the performance of TSA continue unabated. Congressional hearings in the summer of 2016 further solidified these negative perceptions, with the operational head of TSA Melvin Carraway being asked to step down. This termination event is a major rarity in the world of government which often fails to hold people accountable for performance. But TSA, in order to survive, must be customer driven whether it likes it or not since its service is front line with millions of people on a month-to-month basis.



Figure 10.10 A demonstration of a detection dog in action.



Figure 10.11 The seal of TSA.

These same hearings prompted even more calls for legislation allowing the easier and more free flowing return of private sector interests to the TSA function, such as the opt-out program for airport authorities choosing to switch to the private sector over the TSA counterpart.

Known as the Screening Partnership Program, and orchestrated under the direction of TSA, nearly two dozen airport authorities have opted out for private security services.

Internet Exercise: Read and research the SPP legislation and the various processes required at <https://www.law.cornell.edu/uscode/text/49/44920>

See Figure 10.12.¹⁴

10.2.2 Federal Air Marshals

The federal air marshal program plants undercover law enforcement on airline flights. The program operates with specific intelligence or through random flight assignments. Federal air marshals are skilled in the use of weaponry and defense/offense tactics that involve restraint. Marshals must blend in with passengers, keeping any unsuspecting terrorist unaware of his or her presence on that plane. Marshals employ investigative techniques, criminal terrorist behavior recognition, firearms proficiency, aircraft-specific tactics, and close-quarters self-defense measures to protect the flying public (Figure 10.13).

Internet Exercise: Learn more about a career in the Federal Air Marshal Service at <http://www.usmarshals.gov/careers>; See also <https://www.tsa.gov/about/jobs-at-tsa>.

Screening Partnership Program

Since 2004, all federalized airports are eligible to apply to the Screening Partnership Program. The Screening Partnership Program contracts with qualified screening vendors to provide private security screening under TSA oversight at airports nationwide. There are a total of 22 airports that participate in the Screening Partnership Program.

The FAA Reauthorization Act of 2018 set the standards for processing Screening Partnership Program applications. The Act directs TSA to approve an airport operator's application to participate in the Screening Partnership Program if approval will not compromise security, detrimentally affect cost efficiency, or detrimentally affect the screening effectiveness of passengers or property at the airport.

How to Apply

Step 1: Interested airport operators must submit an application to their local federal security director. Application information can be found under the "For Industry" section on tsa.gov.

Step 2: Applicants will receive a notification of application status within 60 days. Once an airport operator application is approved, the procurement and the award process can take approximately up to 120 days.

Step 3: After a contract is awarded, transition into the program may take up to 120 days, as practicable based on airport size.

Important Details

- The screening vendor works for TSA and not the airport authority.
- The Federal Security Director remains in charge of security, incident management, and stakeholder relations.
- TSA monitors vendor performance not vendor staffing levels.
- Private screening vendors must comply with all TSA Standard Operating Procedures, policies, guidelines, enhanced pat-down protocol and the use of Advanced Imaging Technology.
- Private screening vendors must use TSA provided screening technologies and cannot use their own.
- Wait times* are the same whether an airport is privatized or federalized.



* Passenger volume has increased at most large airports. However, the time during which passenger volume increases can impact wait times. If passenger volume increases during non-peak periods, instead of peak periods, then there is a minimal effect on wait times.

Private security screening companies are subject to the same hiring restrictions and challenges as the federal government. Contract security screening candidates receive the same security background and medical checks as prospective federal transportation security officers.



**Transportation
Security
Administration**

Tel: 571-227-2829 / tsamedia@tsa.dhs.gov / visit tsa.gov

Figure 10.12 TSA's Screening Partnership program.

10.2.3 Federal Flight Deck Officers

The Federal Flight Deck Officer (FFDO) program permits aviation pilots to be fully armed in the cockpit. TSA identifies and trains qualified officers for this position. Under this program, eligible flight crew members are authorized by the TSA Office of Law Enforcement/Federal Air Marshal Service to use firearms to defend against an act of criminal violence or air piracy that



Figure 10.13 Federal air marshal patch.

attempts to gain control of an aircraft. A flight crew member may be a pilot, flight engineer, or navigator assigned to the flight. The program is required to maintain strict confidentiality of its participants. The FFDOs are further characterized and empowered by these criteria:

- FFDOs are considered federal law enforcement officers only for the limited purposes of carrying firearms and using force, including lethal force, to defend the flight deck of an aircraft from air piracy or criminal violence.
- FFDOs are not granted or authorized to exercise other law enforcement powers, such as the power to make arrests, or seek or execute warrants for arrest, or seizure of evidence, or to otherwise act as federal law enforcement outside the jurisdiction of aircraft flight decks.
- FFDOs are issued credentials and badges to appropriately identify themselves to law enforcement and security personnel, as required in the furtherance of their mission.
- FFDOs are issued firearms and other necessary equipment by the Federal Air Marshal Service.
- FFDOs are responsible for the readiness and daily security of their firearms, credentials, and equipment.
- FFDOs are authorized to transport secured firearms in any state for a flight on which they are flying to or from as approved by the Federal Air Marshal Service as necessary for their participation and activities in the program.

To be eligible for this position, you must meet the following requirements:

- Pilots
- Flight engineers
- Flight navigators

To be eligible, you must have:

- A current FAA airman certificate
- A current class one or class two medical certificate
- U.S. citizenship

Additionally, individuals must pass a biannual firearms requalification. All eligible flight crew members will attend a 1-week training in Artesia, New Mexico. There is no fee to participate in the Federal Flight Deck Officer program. Training and equipment costs are covered by TSA.¹⁵

10.2.4 Law Enforcement Officers Flying Armed

TSA always oversees a program on instruction and general guidance for law enforcement officers wishing to fly while armed. The program recognizes the critical role a legitimately armed law enforcement officer might play in the event of a terrorist incident. Just as critical is the program's desire to promulgate standards for any law enforcement officer flying on official business. Transporting prisoners, tailing a suspect, or other investigative practice demand an official protocol for the use and storage of firearms. Any officer desiring to fly armed must complete a course of instruction and file the required paperwork giving notice of this intention. Eligibility requirements are:

- Be a federal law enforcement officer or a full-time municipal, county, state, tribal, or territorial law enforcement officer who is a direct government agency employee.
- Be sworn and commissioned to enforce criminal or immigration statutes.
- Be authorized by the employing agency to have the weapon in connection with assigned duties.
- Have completed the TSA Law Enforcement Officer Flying Armed Training Course.¹⁶

Internet Exercise: For a policy directive from TSA on flying armed, see <https://www.tsa.gov/travel/law-enforcement>.

10.2.5 TSA's Canine Explosive Detection Unit

Given the broadening responsibilities of TSA, moving beyond the airports and venturing into seaports, harbors, and train and municipal transit facilities, TSA has had to get creative in how it carries out its task.¹⁷ The use of canines has long been a beneficial and very economical police practice.¹⁸ The use of canines has long been part of the DHS and TSA arsenal.¹⁹ TSA uses canines to detect explosives in various quarters (Figure 10.14).²⁰

Canines are particularly effective in ports and harbor areas, where the sheer volume of coverage area can be daunting for law enforcement. TSA has developed certification standards for canine units for purposes of uniformity and quality in practice.

Internet Exercise: watch the video on canine “REDDI” program at <https://www.dhs.gov/publication/st-reddi-regional-explosives-detection-dog-initiative>

TSA is aggressively developing units and teams throughout the United States. The agency will train and certify more than 400 explosive detection canine teams, composed of one dog and one handler, during the next 2 years. Eighty-five of these teams will be TSA employee led and will primarily search cargo bound for passenger-carrying aircraft. TSA handlers will be non-law-enforcement employees and will complement the 496 TSA-certified state and local law enforcement teams currently deployed to 70 airports and 14 mass transit systems. Currently, there are now 800 various canine teams throughout the United States (Figure 10.15).

Internet Exercise: Find out about the crucial role canines play in the defense of our nation at <https://www.youtube.com/watch?v=AV4I7XNSph0>.

TSA operates a puppy-breeding program to fill the ranks of the future. Volunteers staff the operation and raise puppies who will work in TSA functions. During this time, volunteers provide a well-rounded, socialized, and nurturing environment. TSA delivers an orientation program for volunteers and makes technical staff available during this period of upbringing (Figure 10.16).

Internet Exercise: Find out about the retired dog adoption program that TSA recently announced at <https://www.tsa.gov/news/releases/2015/11/02/tsa-seeking-people-adopt-dogs-who-have-retired-or-have-not-mastered>.

10.2.6 Risk Management Programs

TSA has played an integral role in the development of risk assessment protocols and tools for the transportation system, though not without regular criticism.²¹ Opponents of TSA argue that there is not much thinking going on when it comes to new and innovative protocols. Some

Homeland Security

have said that the agency agrees too quickly to adopting new technology. Even the General Accounting Office (GAO) found that TSA “does not routinely consider costs and benefits when acquiring new technologies.”²²

Despite this, TSA completely appreciates the interrelationship between a risk or series of risks and the critical infrastructure and assets it protects. To understand the risk is to comprehend the

FACTSHEET

TSA Canine Training Center

Overview

The TSA National Explosives Detection Canine Program trains and deploys both TSA-led and state and local law enforcement-led canine teams in support of day-to-day activities that protect the transportation domain. These highly trained explosives detection canine teams are a reliable resource at detecting explosives and provide a visible deterrent to terrorism directed towards transportation systems.

TSA trains canine teams to operate in the aviation, multimodal, maritime, mass transit, and cargo environments. Considered the “center for excellence” for explosives detection canine training, the program is the largest explosives detection canine program in the Department of Homeland Security and the second largest in the federal government after the Department of Defense.



Canine Training Teams

- Canine teams may consist of transportation security inspectors or local or state law enforcement officers who are paired with explosives detection canines and work in airports across the nation.
 - Law enforcement officers make up approximately 65 percent of the teams and approximately 35 percent are transportation security inspectors.
- TSA provides and trains the dog, trains the handler, provides training aides and explosives storage magazines, and conducts annual on-site canine team re-certifications.
- TSA partially reimburses each participating agency for operational costs associated with maintaining the teams, including veterinary fees, handler salaries, dog food, and equipment.
 - In return, the law enforcement agencies agree to use the canines in their assigned transportation environment for at least 80 percent of the handler's duty time.

Canine Training Course

- TSA's explosives detection canines are trained on a variety of explosives based on intelligence data and emerging threats.
- Conventional explosives detection canine handlers undergo a 12-week training course. Passenger screening canine handlers undergo a 16-week training course.
- Canine teams graduate from the TSA canine course after demonstrating proficiency in various venues inclusive of all transportation environments including airport, terminal, freight, cargo, baggage, vehicle, bus, ferry and rail.
- Once a team graduates from the training program, they return to their duty station to acclimate and familiarize the canine to their assigned operational environment.
- Each team is continually assessed to ensure the canines demonstrate operational proficiency in their environment to include four key elements: the canine's ability to recognize explosives odors, the handler's ability to interpret the canine's change of behavior, the handler's ability to conduct logical and systematic searches, and the team's ability to locate the explosives odor source.



Transportation
Security
Administration

Tel: 571-227-2829 / tsamedia@tsa.dhs.gov / visit tsa.gov

Figure 10.14 Information on TSA's canine training center.

(Continued)

Training Facilities

- Located at Joint Base San Antonio-Lackland in San Antonio, Texas, the \$12 million Canine Training Center includes 25,000 square feet of space with seven classrooms, office space that accommodates 140 employees, and a 100-seat auditorium.
- There are 17 indoor venues on the premises that mimic a variety of transportation sites and modes. This includes a cargo facility, an airport gate area, a checkpoint, a baggage claim area, the interior of an aircraft, a vehicle parking lot, a light rail station, a light rail car, an air cargo facility, a mock terminal, and open area searches venues for air scenting.
- Kennels that can accommodate approximately 200 dogs.
- The canine training center also utilizes a variety of training venues in and around the San Antonio area including San Antonio International Airport, local shopping malls, the ATT Center, and the VIA Bus Terminal.

Canines by the Numbers

- **300:** average number of canines that complete training per year
- **240:** average number of canines in training at any given time
- **7:** breeds of canines that are in the program, to include German Shepherds, Labrador Retrievers, German Short-haired Pointers, Wirehaired Pointers, Vizslas, Belgian Malinois, Golden Retrievers
- **\$26,000:** average cost to train a canine a traditional explosives detection canine and handler and \$42,000 for a passenger screening canine and handler
- Approximately **83 percent** of canines graduate from the training program



Canine Capabilities

- There are more than 1,000 TSA canine teams deployed nationwide that are tasked with screening passengers and cargo, and supporting other security missions.
- In 2019, there were more than 300,000 canine utilization hours throughout the nation's transportation system.
- Canine teams work at more than 100 of the nation's airports, mass-transit and maritime systems.
- Canine teams are a highly mobile and extremely efficient explosives detection tool to deter, detect and respond to threats throughout the nation's transportation environments.



Transportation
Security
Administration

Tel: 571-227-2829 / tsamedia@tsa.dhs.gov / visit [tsa.gov](https://www.tsa.gov)

Figure 10.14b (CONTINUED) Information on TSA's canine training center.

landscape to be protected. To comprehend the landscape to be protected surely leads to the identification and mitigation of risk. TSA also recognizes that transportation assets, such as airplanes and tunnels, are part of larger systems, such as the national aviation system or a mass transit system. Taken together, all the individual transportation systems form the national transportation system. Essentially, TSA discerns systems within systems. The behavior of transportation systems



Figure 10.15 An explosive detection canine team screens cargo.



Figure 10.16 TSA puppy-breeding program recruits.

cannot be fully explained by confining observations to individual cars, vessels, and aircraft or fixed infrastructure. As a result, TSA has developed self-assessment tools for maritime, transportation, and mass transit systems.²³ In 2014, TSA modified its approach to risk management by adopting a new methodology: enterprise risk management (ERM) (Figure 10.17).

ERM tries to find appropriate targets rather than attempting to screen the entire universe for threats and harm. The primary goals of ERM are to

- Provide a structured, disciplined, and consistent approach to assessing risk aligned with U.S. Department of Homeland Security guidance.
- Identify strategic risks that threaten TSA's achievement of our long-term objectives and goals, and manage those risks at the enterprise level through the ERSC.
- Ensure that risks are managed in a manner that maximizes the value TSA provides to the nation consistent with defined risk appetite and risk tolerance levels.
- Align our strategy, process, people, technology, and information to support agile risk management.
- Provide greater transparency into risk by improving our understanding of interactions and relationships between risks in support of improved risk-based decision-making.
- Establish clear accountability and ownership of risk.²⁴



Figure 10.17 ERM protocol. (From Transportation Security Administration. ERM policy manual. August 2014, <https://www.aferm.org/wp-content/uploads/2015/10/TSA-ERM-Policy-Manual-August-2014.pdf>.)

Internet Exercise: For a full analysis of the ERM methodology, visit <https://www.aferm.org/wp-content/uploads/2015/10/TSA-ERM-Policy-Manual-August-2014.pdf>.

10.2.7 TSA Technology and Innovation

Cutting-edge technology is a desired end for TSA. The costs of human intelligence versus mechanical versions are always higher, and realizing the volume of TSA activities, the need for high-level technology has never been greater. The world is a very large place to screen, and the human eye is simply incapable of seeing it all. To stay ahead of the terrorist, TSA has developed and employed some incredible technology, again not without some controversy. In air, cargo holds, ports, and harbor shipping, the use of technology will permit TSA to extend its reach.²⁵ Efforts to make this technology more accurate and efficacious are ongoing and constant. All technology has a planning, research, application, and evaluation phase so it is difficult to do things rapidly. But TSA in particular is always interested in the speed of processing.²⁶ A thumbnail review of a few of the more exciting advances is covered in the following.

10.2.7.1 Trace Portals and Their Demise

The use of the trace portal was a highly touted technique for the detection of dangerous items, such as explosives and anthrax. The portals were allegedly capable of detecting trace, minute quantities of many materials including explosives. From 2007 to 2011, the machines were installed at a host of airports. As passengers entered the trace portal, standing still for a few seconds, several puffs of air are released, dislodging microscopic particles from passengers that are then collected and analyzed for traces of explosives. TSA installed trace portals in Baltimore; Boston; Gulfport, Mississippi; Jacksonville, Florida; Las Vegas; Los Angeles; Miami; Newark; New York (JFK); Phoenix; Providence, Rhode Island; Rochester, New York; San Francisco; San Diego; and Tampa, Florida. See Figure 10.18 for a trace portal.



Figure 10.18 Trace portal.

Unfortunately, the machines proved so ineffective and unpredictable that TSA slowly but surely withdrew the technology, commencing in 2011. With nearly 200 machines in place at a cost of nearly \$30,000,000 million, the program represents another public relations problem for the agency.

10.2.7.2 Millimeter Wave/Advanced Imaging Technology

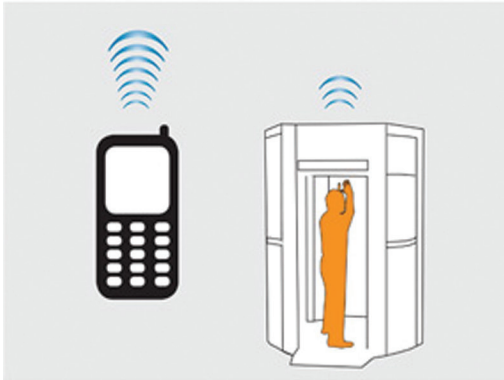
The new means for discerning explosives, improvised explosive devices (IEDs), and other concealed materials are the *millimeter-wave device* and *advanced imaging technology* (AIT). TSA currently uses both types at 78 airports. Around 500 AIT and 300-millimeter wave machines are presently in use (Figure 10.19).

Millimeter-wave imaging technology uses harmless electromagnetic waves to detect potential threats. Beams of radio frequency (RF) energy in the millimeter-wave spectrum are projected



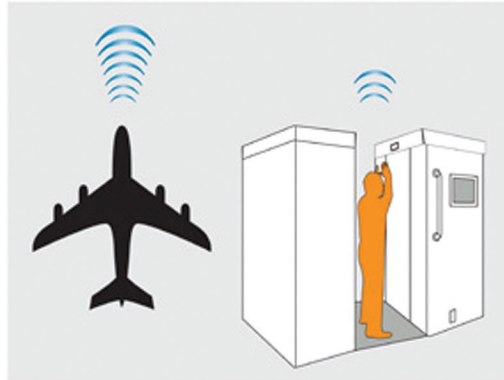
Figure 10.19 AIT machine: the millimeter wave unit.

Millimeter Wave Safety



Millimeter wave technology emits thousands of times less energy than a cell phone transmission.

Backscatter Safety



One backscatter technology scan produces the same exposure as two minutes of flying on an airplane.

Figure 10.20 AIT safety information from TSA. (https://www.tsa.gov/graphics/images/approach/ait_safety_demo.jpg.)

over the body's surface at high speed from two antennas simultaneously rotating around the body. The RF energy reflected back from the body or other objects on the body constructs a three-dimensional image. The three-dimensional image of the body, with facial features blurred for privacy, is displayed on a remote monitor for analysis. The machine itself is innocuous. Earlier imagery lacked specificity relative to identity and hence could not be used for illicit purposes.

However, more modern AIT machines provide exquisite detail as to the physical features and, as a result, have been the subject of some passenger abuse. The resulting images are labeled *backscatter*. Backscatter technology projects an ionizing x-ray beam over the body surface at high speed. The reflection, or backscatter, of the beam is detected, digitized, and displayed on a monitor.

Both systems have generated a stir of comment and criticism. For some, the safety of the imagery and its mechanics trump the safety of the general public. If the technology utilizes waves, in whatever form, critics indicate there may be health risks. TSA has taken these critiques seriously and tried to calm the public by making comparisons. For example, the exposure to waves during a backscatter scan is like flying a plane for 2 minutes, while those experienced during a millimeter-wave scan are similar to using a cell phone (Figure 10.20).

In addition, the machines cannot sensibly differentiate common medical devices that are absolutely innocent by design, such as an insulin pump monitor for diabetics, pacemakers for heart conditions, and neurostimulators for neurological problems. As such, since the machines tend to lump the common terrorist together with the sickly patient, this likewise causes a further erosion of trust regarding TSA.²⁷

Internet Exercise: Read about the various health assessments that have been done on AIT at http://www.dhs.gov/sites/default/files/publications/tsa-safety-study-ait-info-memo_0.pdf.

Even more common has been the privacy challenge to intrusive machinery.²⁸ AIT and millimeter-wave machines peer deep into the private range of human operations. Balancing the rationale of safe travel with minimal intrusiveness may be less compelling than the searched bag comparison. Surely, every traveler realizes that privacy concerns are not idyllic and untouchable. In a post-9/11 world, most people accept the burdens and inconveniences of security checkpoints.

Internet Exercise: See how TSA portrays its version of the imaging technology at <https://youtu.be/AXtZoQLQ9p4>.

Even so, the intrusiveness has limits and this machinery may have reached the threshold where the public's patience runs out. TSA has some sensitivity to privacy concerns.²⁹ It has

Homeland Security

altered the imagery to a generic format that cannot personally be identified, it has the screener in a distinct position from the officer assisting the customer, and it has assured that imagery cannot be stored, printed, transmitted, or saved.³⁰

The agency has modified its software packages to show a generic figure that lacks specificity. Known as *automated target recognition*, ATR eliminates the image of the individual body while still recognizing anomalies.³¹ See Figure 10.21 for an ATR image.

Granting the intrusiveness of these technologies, the price of that intrusion may be worth the results in weaponry confiscation alone;³²

More recently, airport screening has experimented with hospital equipment—MRI like and labeled computed tomography.³³ This new technology provides vivid, 3D imagery that is more effective in ferreting out contraband and weaponry. See Figure 10.22.

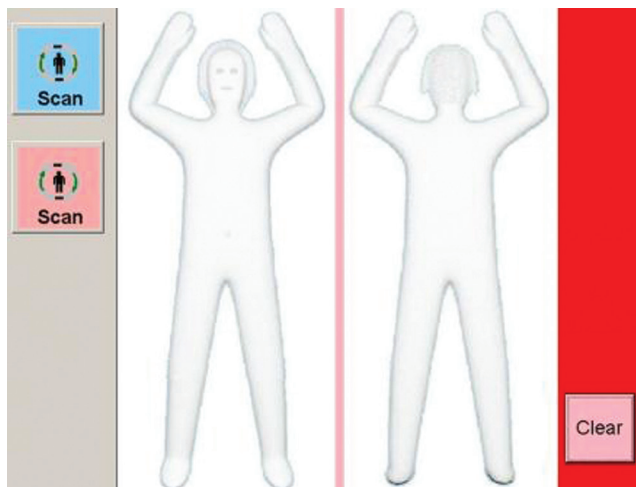


Figure 10.21 TSA is using software that enhances privacy by highlighting any potential threats on the same generic outline of a person for every passenger. (From Transport Security Administration, <https://www.tsa.gov/>.)



Figure 10.22 A baggage screen tomography machine. (Source: TSA.)

TSA is currently using this advanced technology at the following airports:

- Hartsfield-Jackson Atlanta International Airport (ATL)
- Baltimore-Washington International Airport (BWI)
- Chicago O'Hare International Airport (ORD)
- Cincinnati/Northern Kentucky International Airport (CVG)
- Detroit Metropolitan Wayne County Airport (DTW)
- Houston Hobby Airport (HOU)
- Indianapolis International Airport (IND)
- John F. Kennedy International Airport (JFK)
- Logan International Airport (BOS)
- Los Angeles International Airport (LAX)
- Miami International Airport (MIA)
- Oakland International Airport (OAK)
- Phoenix Sky Harbor International Airport (PHX)
- Ronald Reagan Washington National Airport (DCA)
- St. Louis Lambert International Airport (STL)
- Tampa International Airport (TPA)
- Washington-Dulles International Airport (IAD)

10.2.7.3 Biometrics

The world of *biometrics* has clearly invaded the day-to-day life of TSA. Biometrics can be defined as follows:

- Biometrics is a general term used alternatively to describe a characteristic or a process.
- As a characteristic, a biometric is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.
- As a process, a biometric is an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.³⁴

Biometrics is a means of identification using both machine and man.³⁵ Presently, biometrics can target various bodily components for identification, including:

- Palm
- Fingerprint
- Face
- Vascular system
- Speech
- Eye

Both retinal scans and fingerprint analysis by digital means are available to the agency. Biometric fingerprint machines are becoming a common experience for both residential and international travelers (Figure 10.23). Facial recognition machines are increasingly becoming part of the transportation landscape.³⁶ Machines that trace and match retinal patterns are sure to grow just as quickly.³⁷



Figure 10.23 Biometric fingerprint scanner.

10.2.7.3.1 Biometric Application: The Trusted Traveler Program

Biometric applications are becoming very common in the travel and transportation industries. The FBI has taken the lead on the various modalities relating to biometric applications by and through its Biometric Center of Excellence (Figure 10.24).³⁸

All of these new technologies hope to speed up the travel process and may or may not use biometric applications. Early on, TSA created the Registered Traveler (RT) program in an effort to speed up the traveling process for business and repeat travelers. The program has recently been lumped together with other programs under the banner Trusted Traveler. See the included programs in Figure 10.25.³⁹

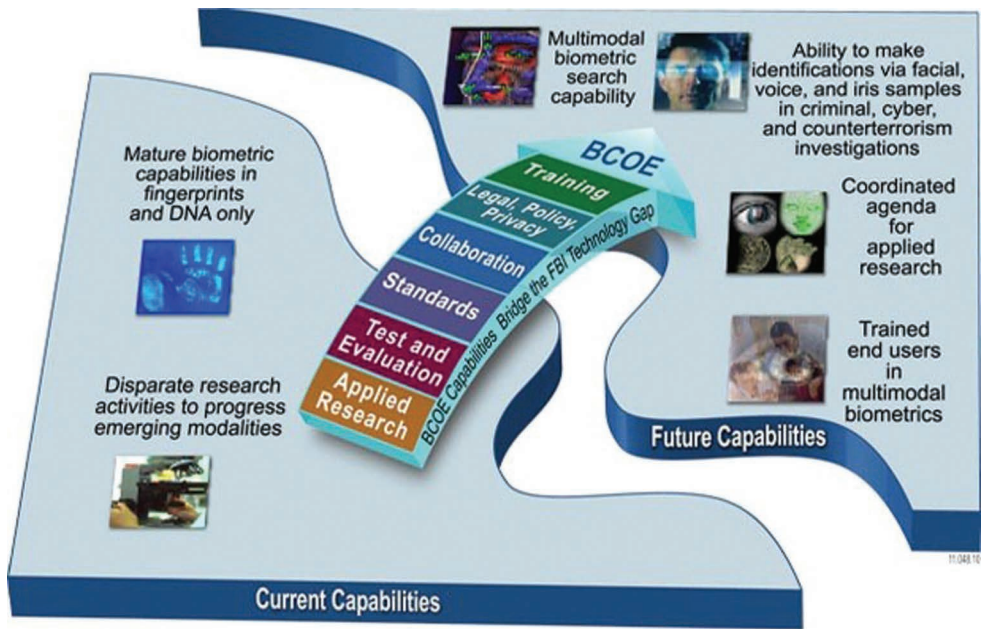


Figure 10.24 Various biometric modalities.

10.2 Transportation Security Administration

Trusted Traveler Programs

Welcome to the official U.S. Department of Homeland Security website, where travelers can apply for Trusted Traveler Programs. Our programs allow members to use expedited lanes at the U.S. airports, and when crossing international borders.

Choose a Program to Get Started

All memberships are valid for 5 years

Departures from U.S. Airports \$85 USD Travel by Air Eligibility U.S. citizens and U.S. lawful permanent residents Learn More Get Started	Entry into the U.S. from International Destinations \$100 USD Travel by Air, Land and Sea Includes TSA Pre✓ Eligibility U.S. citizens, U.S. lawful permanent residents, and select foreign nationals Learn More Get Started	Entry into the U.S. from Canada \$50 USD Travel by Air, Land and Sea may include TSA Pre✓ Eligibility U.S. citizens, U.S. lawful permanent residents, Canadian citizens, Canadian permanent residents, and Mexican nationals Learn More Get Started	Entry into the U.S. from Canada and Mexico \$122.50 USD Travel by Air and Land may include TSA Pre✓ Eligibility U.S. citizens, U.S. lawful permanent residents and all foreign nationals. Learn More Get Started	For truck drivers entering and exiting the U.S. from Canada and Mexico \$50 USD Travel for Commercial Trucks does not include TSA Pre✓ Eligibility U.S. citizens, U.S. lawful permanent residents, Canadian citizens, Canadian permanent residents, and Mexican nationals Learn More Get Started
--	--	--	---	---

The **Trusted Traveler Programs** (Global Entry, TSA Pre✓®, SENTRI, NEXUS, and FAST) are risk-based programs to facilitate the entry of pre-approved travelers. All applicants are vetted to ensure that they meet the qualifications for the program to which they are applying. Receiving a 'Best Match' or program recommendation based on eligibility or travel habits does not guarantee acceptance into any Trusted Traveler program.

Figure 10.25 Information on DHS's Trusted Traveler program.

In order to participate, passengers undergo a TSA-conducted security threat assessment (STA). It is a voluntary program with both corporate entities and individuals participating. Biometrics plays a key role in this program. To enroll, applicants voluntarily provide Trusted Traveler-sponsoring entities (participating airports/air carriers) and service providers with biographic and biometric data needed for TSA to conduct the STA and determine eligibility. To date, the following agencies participate in the Trusted Traveler program.

ALABAMA

Huntsville (Huntsville Enrollment Center)

Mobile (Mobile Enrollment Center)

ALASKA

Anchorage (Anchorage Enrollment Center)

Fairbanks (Fairbanks Enrollment Center)

ARIZONA

Douglas (Douglas Enrollment Center)

NOGALES (Nogales Enrollment Center)

Phoenix (Phoenix Sky Harbor Global Entry Enrollment Center)

Homeland Security

San Luis (San Luis Enrollment Center)

Tucson (Tucson Enrollment Center)

CALIFORNIA

Calexico (Calexico Enrollment Center)

Long Beach (Permanently Closed)

LOS ANGELES (Los Angeles International Global Entry EC)

San Diego (San Diego–Otay Mesa Enrollment Center)

San Francisco (SF Enrollment Center)

COLORADO

Denver (Denver International Airport)

CONNECTICUT

Windsor Locks (Hartford, CT Enrollment Center)

DISTRICT OF COLUMBIA

Washington (Ronald Reagan BLD)

FLORIDA

Fort Pierce (Treasure Coast Intl. Airport)

Ft Lauderdale (Fort Lauderdale Global Entry Enrollment Center)

Miami (Miami International Global Entry EC)

Orlando (Orlando Global Entry Enrollment Center)

Riviera Beach (West Palm Beach Enrollment Center)

Sanford (Sanford Global Entry Enrollment Center)

Tampa (Tampa Enrollment Center)

GEORGIA

Atlanta (Atlanta International Global Entry EC)

Atlanta (Atlanta Port Office Global Entry Enrollment Center)

GUAM

Tamuning (Guam International Airport)

HAWAII

Honolulu (Honolulu Enrollment Center)

IDAHO

Boise (Boise Enrollment Center)

ILLINOIS

CHICAGO (Chicago O'Hare International Global Entry EC)

CHICAGO

Moline (Moline Quad Cities International Airport)

Peoria (Peoria International Airport)

Rockford (Rockford-Chicago International Airport)

INDIANA

South Bend (South Bend Int'l Airport)

KENTUCKY

Erlanger (Cincinnati Enrollment Center)

LOUISIANA

Kenner (New Orleans Enrollment Center)

MAINE

Calais (Calais Enrollment Center)

MARYLAND

Linthicum (Baltimore Enrollment Center)

MASSACHUSETTS

East Boston (Boston-Logan Global Entry Enrollment Center)

MICHIGAN

Detroit (Detroit Enrollment Center)

Detroit (Detroit Metro Airport Global Entry)

Port Huron (Port Huron Enrollment Center)

Sault Ste. Marie (Sault Ste Marie EC)

MINNESOTA

Grand Portage (Grand Portage GE EC)

International Falls (International Falls Enrollment Center)

International Falls (International Falls Global Entry Enrollment Center)

St. Paul (Minneapolis -St. Paul Airport)

Warroad (Warroad Enrollment Center)

MISSISSIPPI

Gulfport (Gulfport-Biloxi Global Entry Enrollment Center)

Homeland Security

MISSOURI

Kansas City (Kansas City Enrollment Center)

St. Louis (St. Louis Enrollment Center)

MONTANA

Sweetgrass (Sweetgrass NEXUS and FAST)

Sweetgrass (Sweetgrass Global Entry)

NEVADA

Las Vegas (Las Vegas Enrollment Center)

NEW JERSEY

Newark (Newark Global Entry Enrollment Center)

NEW MEXICO

Albuquerque (Albuquerque Enrollment Center)

NEW YORK

Albany (Albany International Airport)

Champlain (Champlain Enrollment Center)

Jamaica (JFK International Global Entry EC)

NEW YORK (Bowling Green)

NIAGARA FALLS (Niagara Falls EC)

NORTH CAROLINA

Charlotte (Charlotte-Douglas Airport)

NORTH DAKOTA

Grand Forks (Grand Forks Enrollment Center)

Pembina (Pembina Enrollment Center)

Pembina (Pembina Global Entry Enrollment Center)

OHIO

Middleburg Heights (Cleveland U.S. Customs and Border Protection)

Port Clinton (Port Clinton, Ohio Enrollment Center)

Vandalia (Dayton Enrollment Center)

OREGON

Portland (Portland, OR Enrollment Center)

PENNSYLVANIA

PHILADELPHIA (Philadelphia Global Entry Enrollment Center)

Pittsburgh (Pittsburgh International Airport)

PUERTO RICO

Carolina (San Juan Global Entry Enrollment Center)

RHODE ISLAND

Warwick (Warwick, RI Enrollment Center)

TENNESSEE

Blountville (Tri-Cities Enrollment Center)

Memphis (Memphis International Airport Global Enrollment Ce)

Nashville (Nashville Enrollment Center)

TEXAS

Austin (Austin-Bergstrom International Airport)

Brownsville (Brownsville Enrollment Center)

DFW Airport (Dallas-Fort Worth Intl Airport Global Entry)

Eagle Pass (Eagle Pass Enrollment Center)

El Paso (El Paso Enrollment Center)

Houston (Houston Intercontinental Global Entry EC)

Houston (Houston Term E-BOARDING PASS REQUIRED TO ENT)

Laredo (Laredo Enrollment Center)

Mission (Hidalgo Enrollment Center)

San Antonio (San Antonio International Airport)

UTAH

Salt Lake City (Salt Lake City International Airport)

VERMONT

Derby Line (Derby Line Enrollment Center)

VIRGINIA

Richmond (Richmond, VA Enrollment Center)

Sterling (Washington Dulles International Global Entry EC)

WASHINGTON

Blaine (Blaine Global Entry Enrollment Center)

Seattle (SeaTac International Airport Global Entry EC)

WISCONSIN

Milwaukee (Milwaukee Enrollment Center)⁴⁰



Figure 10.26 An example of a paperless boarding pass as it appears on a smartphone.

Internet Exercise: Visit the Trusted Traveler website and use their comparison tool to find the best program for your traveling needs at <https://tftp.dhs.gov/>

10.2.7.3.2 TSA Paperless Boarding Pass

In an effort to streamline security processes and to assure a free flow of traffic in congested airports, TSA has implemented a paperless boarding pass program. Here, the passenger downloads the boarding pass to a cell phone or other device and scans it at a designated station. Currently, most airports have adopted the program. Using a scan code, the TSA agent verifies the pass by a mere swipe (Figure 10.26).

The program has been favorably received by the general public, though there are the usual caveats about privacy issues and the sharing of this personal information. TSA has issued strict guidelines on privacy requirements and reigned in the technology to prevent unauthorized disclosure.⁴¹

There is much more that could be written concerning the activities of TSA. Throughout the remainder of this chapter, the role of TSA in other aspects involving the transportation industry will be highlighted. In fact, our coverage turns to two key areas in the transportation arena: maritime and rail.

10.3 Maritime Security

Maritime security is an interagency operation at the federal level, with the prime players being the Coast Guard, Customs and Immigration Service, and DHS. In 2011, DHS announced a more formal association of the major players in maritime security titled the Marine Operations Coordination (MOC) plan. MOC will coordinate and plan for the integration of maritime operations of the U.S. Coast Guard, CBP, and Immigration and Customs Enforcement. The MOC plan focuses on improved collaboration across five key sectors.

- Coordination
- Planning
- Information sharing
- Intelligence integration
- Response activities

10.3 Maritime Security

DHS has also fostered interagency cooperation in maritime threat affairs by the creation of the Maritime Operational Threat Response (MOTR) program. The primary aim of the program is to coordinate all relevant agencies of government that might encounter maritime threats and to assure the free flow of information to all interested agencies. A schematic of how all agencies report to MOTR is in Figure 10.27.

Previous to 9/11, conceptions of maritime security largely dealt with smuggling, theft, and drug trafficking.⁴² Since that time, maritime security has been evaluated in more global terms. Maritime enforcement can only be described as a major undertaking that draws in all sectors of defense, including the traditional branches of the armed services.⁴³

The maritime domain is defined as all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels, and other conveyances. The maritime domain for the United States includes the Great Lakes and all navigable inland waterways, such as the Mississippi River and the Intracoastal Waterway.

In the most general terms, maritime security seeks to accomplish the following ends:

- Prevent terrorist attacks and criminal or hostile acts
- Protect maritime-related population centers and critical infrastructures
- Minimize damage and expedite recovery
- Safeguard the ocean and its resources

The Maritime Security Transportation Act of 2002 was the initial legislative response after the attack of 9/11.⁴⁴ The act requires vessels and port facilities to conduct vulnerability assessments and develop security plans that may include passenger, vehicle, and baggage screening procedures, security patrols, establishing restricted areas, personnel

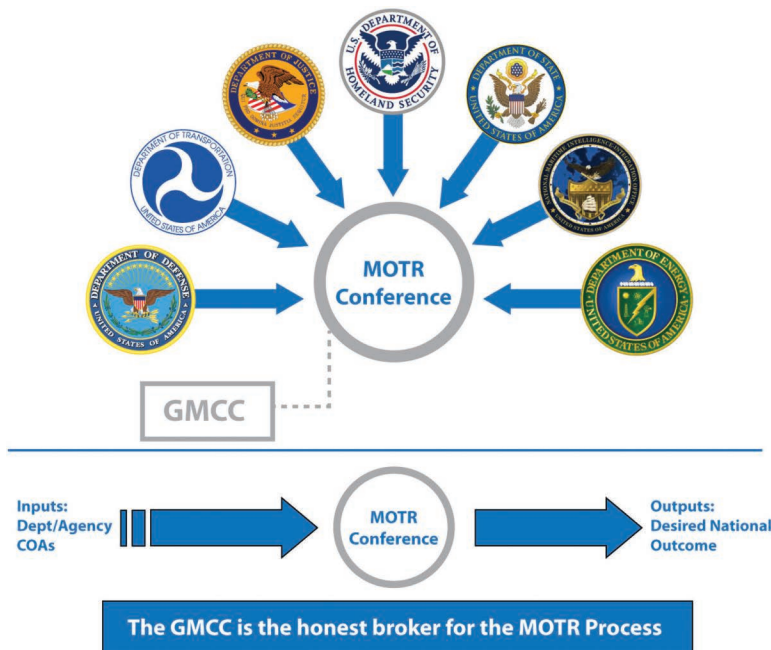


Figure 10.27 Maritime operational threat response process.

Homeland Security

identification procedures, access control measures, and installation of surveillance equipment. Developed using risk-based methodology, the security regulations focus on those sectors of maritime industry that have a higher risk of involvement in a transportation security incident, including various tank vessels, barges, large passenger vessels, cargo vessels, towing vessels, offshore oil and gas platforms, and port facilities that handle certain kinds of dangerous cargo or service these vessels.

Internet Exercise: For the entire language of the act, see <https://www.gpo.gov/fdsys/pkg/PLAW-107publ295/pdf/PLAW-107publ295.pdf>.

10.3.1 National Strategy for Maritime Security

The complexities of maritime security arise from geography, legal issues, and a host of competing agencies and departments who have some portion of the pie—for example, defense, energy, interior, state, and DHS. Matters of territorial waters can be daunting and any effort to secure the homeland must weigh these competing interests.

In 2005, DHS published its National Strategy for Maritime Security.⁴⁵ The national strategy hones in on these fundamental objectives:

- Detect, deter, interdict, and defeat terrorist attacks, criminal acts, or hostile acts in the maritime domain, and prevent its unlawful exploitation for those purposes.
- Protect maritime-related population centers, critical infrastructure, key resources, transportation systems, borders, harbors, ports, and coastal approaches in the maritime domain.
- Define and set out the maritime domain.
- Minimize damage and expedite recovery from attacks within the maritime domain.
- Safeguard the ocean and its resources from unlawful exploitation and intentional critical damage.
- Enhance international cooperation to ensure lawful and timely enforcement actions against maritime threats.
- Embed security into commercial practices to reduce vulnerabilities and facilitate commerce.
- Deploy layered security to unify public and private security measures.
- Ensure continuity of the marine transportation system to maintain vital commerce and defense readiness.

The national strategy fully accepts that the world's waterways depend on extraordinary cooperation at both the national and international levels. Any strategy must balance commerce with defense considerations, international rights with sovereignty of the coastline, and with the full recognition that certain bodies of water are internationally accessible while others are protected. Figure 10.28 portrays all these dynamics.

Both government and commercial interests need to work together. Nations and states must coordinate response and action and adopt common definitions and parameters for what constitutes the maritime domain. The National Strategy on Maritime Security realizes the complexity of protecting the world's seas and waterways. It realizes that governmental entities and bodies need coordination. As a result, the strategy erects the Interagency Maritime Security Policy Coordinating Committee, established to serve as the primary forum for coordinating U.S. government maritime security policies. The committee reviews existing interagency practices, and coordination and execution of U.S. policies and strategies relating to maritime security, and recommends improvements, as necessary.

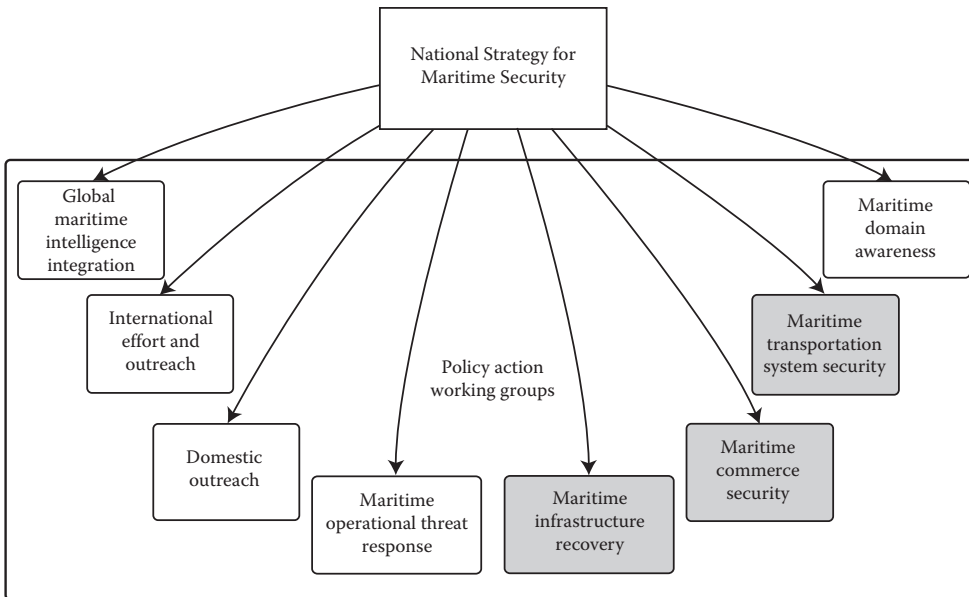


Figure 10.28 National strategy for maritime security.

10.3.2 Other Maritime Plans

At the national level, there are eight other plans or programs dedicated to the protection of the maritime domain—namely:

- The National Plan to Achieve Maritime Domain Awareness lays the foundation for an effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States.
- The Maritime Transportation System Security Plan responds to the president's call for recommendations to improve the national and international regulatory framework regarding the maritime domain.
- The Maritime Commerce Security Plan establishes a comprehensive plan to secure the maritime supply chain.
- The Maritime Infrastructure Recovery Plan recommends procedures and standards for the recovery of the maritime infrastructure following attack or similar disruption.
- The International Outreach and Coordination Strategy provides a framework to coordinate all maritime security initiatives undertaken with foreign governments and international organizations.
- The Global Maritime Intelligence Integration Plan uses existing capabilities to integrate all available intelligence regarding potential threats to U.S. interests in the maritime domain.
- The Maritime Operational Threat Response Plan aims for coordinated U.S. government response to threats against the United States and its interests in the maritime domain by establishing roles and responsibilities.
- The Domestic Outreach Plan engages nonfederal input to assist with the development and implementation of maritime security policies.

Space limitations prevent full coverage of each of the plans, but it shall be sufficient to cover the more prominent ideas in maritime security.

10.3.2.1 National Plan to Achieve Maritime Domain Awareness

The National Plan to Achieve Maritime Domain Awareness educates the public about the nature of a maritime domain in order that threats may be identified. Maritime domain awareness involves anything associated with the global maritime domain that could impact the United States' security, safety, economy, or environment. A range of federal departments and agencies will need to coordinate closely to identify threats as early and as distant from our shores as possible. By unifying U.S. government efforts and supporting international efforts, this plan will help achieve maritime domain awareness across the federal government, with the private sector and civil authorities within the United States, and with our allies and partners around the world.⁴⁶

10.3.2.2 Maritime Transportation System Security Plan

The Maritime Transportation System (MTS) Security Plan seeks to improve the national and international regulatory framework regarding the maritime domain. The MTS evaluates maritime security in light of its various systems. The MTS is a network of maritime operations that interface with shore-side operations at intermodal connections as part of overall global supply chains or domestic commercial operations. The various maritime operations within the MTS operating network have components that include vessels, port facilities, waterways and waterway infrastructure, intermodal connections, and users. DHS will issue a series of continuing recommendations regarding the safety of the network and its various components.

What is undeniable is that terrorists have attempted to use terrorism in the maritime domain. Professionals from all branches of defense and law enforcement constantly watch the horizon for new means and methods of attacks.

10.3.3 DHS: Borders and Marine Division

The long-held view that cargo and port inspections were the exclusive province of the U.S. Coast Guard has been set aright since 9/11. Multiple agencies of government are now taking on active roles to assure the safety and security of what comes in and what goes out. Discussed throughout this chapter is the role of the Border Division and its many dedicated employees. DHS, by and through its Border and Marine Division, takes these activities to a higher plane. Marine security does not end when the ship docks but is simply at another layer of scrutiny. Cargo, containers, cartons, and supplies stowed on these vessels are part of that secure continuum. While the Coast Guard interdicts and inspects, it cannot be stretched much thinner than its present state. Hence, the work of DHS in this critical area fills a crucial void in assuring the flow of goods and the safe environment the public expects. A thumbnail sketch of the more relevant projects follows.

The Advanced Container Security Device (ACSD) project involves developing an advanced sensor system for monitoring a container's integrity from the point of consolidation to the point of deconsolidation in the maritime supply chain. The ACSD is a small unit that attaches to the inside of a container to monitor all six sides to report any intrusion or door opening, including the presence of human cargo in the container. If the ACSD detects an intrusion, it will transmit this alarm information through the Marine Asset Tag Tracking System (MATTS) to CBP. The ACSD would also build in a standard plug-and-play interface capability so that users can easily integrate other security or commercial sensors (e.g., radiological/nuclear and chemical/biological) through the standard interface.

The CanScan project is developing a next-generation nonintrusive inspection (NII) system that will be used to detect terrorist materials, contraband items (e.g., drugs, money, illegal firearms), and stowaways at border crossings, maritime ports, and airports. These new systems may provide increases in penetration, resolution, and throughput, and will support marine containerized cargo as well as airborne break-bulk, palletized, and containerized cargo; CanScan will provide improved cargo screening.

The Container Security Device (CSD) project is developing a security device with sensors that can detect the opening of container doors from the point of consolidation to the point of

deconsolidation in the maritime supply chain. The CSD will provide an interim capability to monitor the status of container doors until the ACSD is available. The CSD is a small, low-cost device mounted on or within a container that detects the opening or removal of container doors and reports its status to CBP.

The Hybrid Composite Container project is developing a next-generation International Standards Organization (ISO) composite shipping container with embedded security sensors to detect intrusions from the point of consolidation to the point of deconsolidation in the maritime supply chain. Composites are stronger than steel, 10%–15% lighter than current shipping containers, and are easier to repair. Weight savings can benefit shippers by allowing them to load more goods per container within weight limits.

The MATTS project is establishing a remote, global communications and tracking network that works with ACSD from the point of consolidation to the point of deconsolidation in the maritime supply chain. MATTS communicates security alert information globally through the use of RF, cellular, and satellite technology. In addition, the commercial shipping industry can track and monitor cargo as it moves through the supply chain.

The Secure Carton project develops technology to detect any shipping carton tamper event and transmit an alert to authorities after it leaves the point of manufacture to the point that it is delivered in the supply chains. This project provides improved supply chain visibility, chain of custody, and security. It is scalable and applicable across the various shipping modalities, including trucking, rail, maritime, and air cargo.

The Secure Wrap project provides a transparent, flexible, and tamper-indicative wrapping material to secure and monitor palletized cargo after it leaves the point of manufacture to the point of delivery in the land, maritime, and air cargo supply chains. The wrap will provide a visible and/or fluorescent tamper indication and is deployable with little or no impact to current supply chain logistics and processes. Subsequent iterations of this wrap will support increasing levels of automated monitoring, thereby reducing the manpower required to ensure cargo integrity.

10.3.4 Role of the Coast Guard in Maritime Security

At sea and on the continental shelf, in major lakes and rivers, the U.S. Coast Guard assumes the preeminent role in maritime security. With its fleet of cutters and world-class tugs and rescue vessels, high-level technology, skill in port and harbor investigations, and a professional class of officers and staff, it is difficult to find a better fit (Figure 10.29).

The goals, aims, and purposes of the United States Coast Guard are multi-dimensional and are charted in Figure 10.30.⁴⁷



Figure 10.29 U.S. Coast Guard patrol vehicles. (Source: USCG.)

Homeland Security

Mission

The mission of the United States Coast Guard is to ensure our Nation's maritime safety, security and stewardship.

Vision

Ready

We will be prepared to serve and protect the American people and our national interests.

Relevant

We will be a professional and agile armed force, law enforcer, regulator, and maritime first responder on which our partners confidently rely to address the Nation's increasingly complex maritime challenges.

Responsive

We will employ our bias for action to excel in mission execution as we protect and defend the homeland.

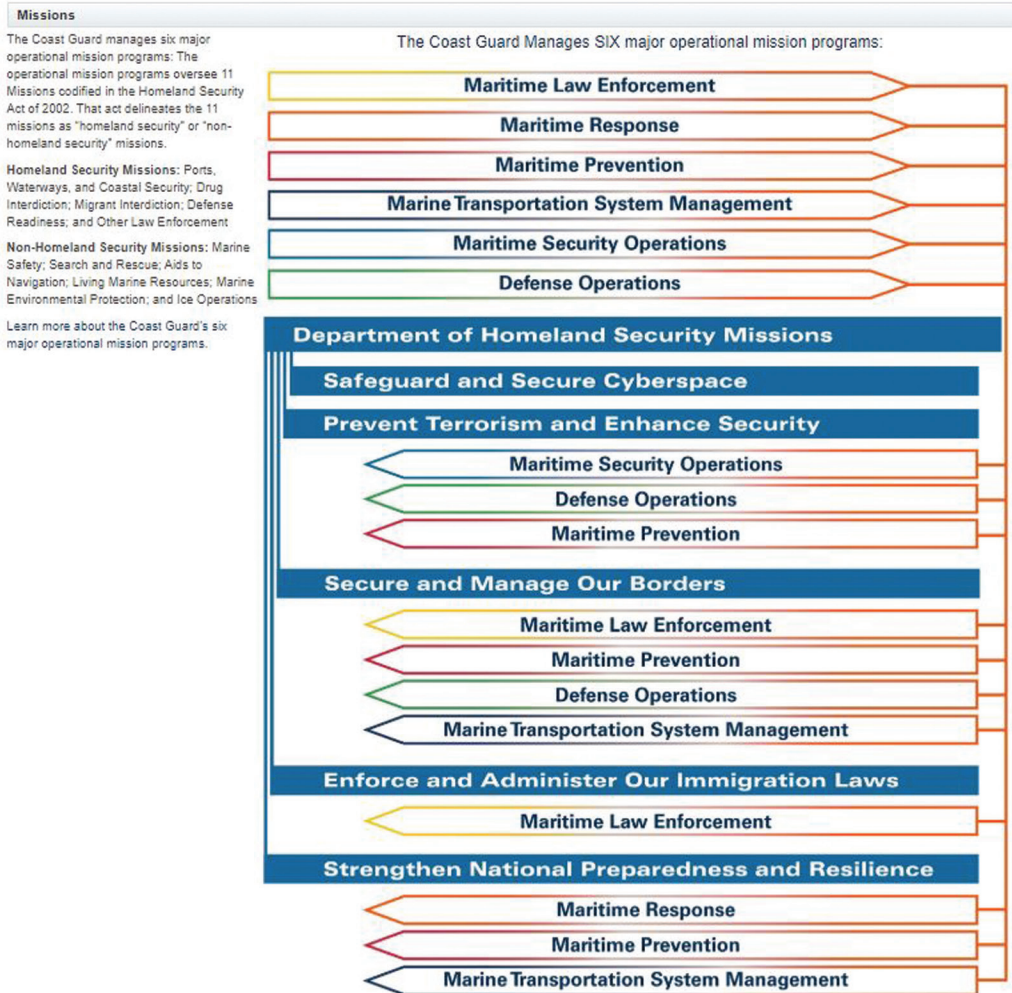


Figure 10.30 The U.S. Coast Guards stated mission, vision, and six operational vision programs.

At its heart, the Coast Guard's central mission always relates to maritime activities and safety and security in the maritime setting. Many of the tasks are listed below.

- Ports, waterways, and coastal security
- Drug interdiction

- Aids to navigation
- Search and rescue
- Living marine resources
- Marine safety
- Defense readiness
- Migrant interdiction
- Marine environmental protection
- Ice operations
- Other law enforcement

With this multifaceted mission in mind, it is no wonder that the Coast Guard so actively intervenes in the day-to-day operations of the maritime sector and it is equally not surprising that the Coast Guard is severely starved for resources to carry out the depth and breadth of these mission areas. Examples of Coast Guard roles and functions in the maritime world are myriad.

10.3.4.1 Emergency Safety

The effectiveness and professionalism of the Coast Guard can always be gleaned from their role in emergency response. Coast Guard assistance in times of storms, hurricanes, floods, and other natural disasters is the stuff of legend (Figure 10.31).

Throughout its distinguished history, the Coast Guard has more than saved lives: it has also rescued whole communities. At no place was this more obvious than during Hurricane Katrina. Referred to as the only shining moment and silver lining in the debacle, Coast Guard personnel swept up person after person in the raging waters of New Orleans. The Coast Guard single-handedly saved more residents of New Orleans than any other governmental authority (Figure 10.32).

Wherever water runs, the Coast Guard is always prepared and ready to serve those in distress. From Hatteras, North Carolina, beaches to Lake Superior, maritime safety comes first for this service.



Figure 10.31 The U.S. Coast Guard is instrumental in saving lives.



Figure 10.32 Coast Guard over New Orleans after Hurricane Katrina.



Figure 10.33 Search and rescue patch.

The most prominent safety unit in the Coast Guard is its search and rescue (SAR) team (Figure 10.33).

The primary goal of SAR is to minimize the loss of life to those in distress, and the Coast Guard saves more than 85% of those who call. When one evaluates the locations of these dangerous rescues, it is simply an extraordinary statistic. The Coast Guard employs a formula to account for the effectiveness in mitigating the loss of life.⁴⁸

$$= \frac{LS}{(LS + (LLB + LLA + LUF))} \quad (10.1)$$

where:

LS=lives saved

LLB=lives lost before notification

LLA=lives lost after notification

LUF=lives unaccounted for (or missing), as defined and input into Marine Information for Safety and Law Enforcement (MISLE)

Internet Exercise: Read about the SAR program at the Coast Guard website at <https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Response-Policy->



Figure 10.34 Coast Guard SAR team member at training.

CG-5R/Office-of-Incident-Management-Preparedness-CG-5RI/US-Coast-Guard-Office-of-Search-and-Rescue-CG-SAR/.

The SAR program is physically demanding and recruits experience a significant attrition rate of nearly 80%. Check with your local Coast Guard recruiter on eligibility standards (Figure 10.34).

Internet Exercise: To learn about the curriculum and the physical demands leading to high attrition rates, see <http://www.defenselink.mil/news/-newsarticle.aspx?id=25362>.

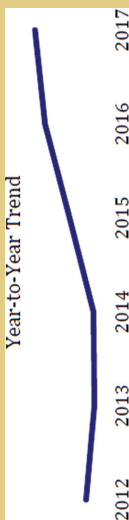
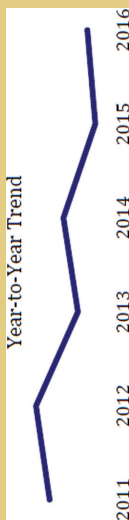
10.3.4.2 Security and Law Enforcement

Law enforcement functions constitute a major portion of Coast Guard activity. In a way, the Coast Guard polices the waters for a host of things, from smuggling to drugs, from illegal human cargo to WMDs. On the water and in the ports, one discovers the critical role of the Coast Guard. The Coast Guard is the law of the sea and waterways.

The Coast Guard is the lead federal agency for maritime drug interdiction. In conjunction with the U.S. Customs Service, the Coast Guard combats and interdicts illegal drugs, interferes with and deters the activities of smugglers using the maritime for illegal delivery of drugs, and engages those that seek to pollute our cities and towns with contraband. Over the last decade, Coast Guard activity in the area of drug interdiction has been active. The Coast Guard's cocaine runs are now becoming the stuff of legend with results captured each year. See the date in Table 10.1.⁴⁹

The Coast Guard has dramatically reoriented its mission to the law enforcement model. The Coast Guard law enforcement mission is statutorily outlined in these general terms:

The Coast Guard shall enforce or assist in the enforcement of all applicable Federal laws on, under, and over the high seas and waters subject to the jurisdiction of the United States; shall engage in maritime air surveillance or interdiction to enforce or assist in the enforcement of the laws of the United States; shall administer laws and promulgate and enforce regulations for the promotion of safety of life and property on and under the high seas and waters subject to the jurisdiction of the United States covering all matters not specifically delegated by law to some other executive department; shall develop, establish, maintain, and operate, with

Table 10.1 The Coast Guard's Statistics of Cocaine Recovered, 2012 through 2018																														
Metric Tons of Cocaine Removed																														
Year-to-Year Trend <table><tr><th>Year</th><th>Metric Tons</th></tr><tr><td>2012</td><td>107</td></tr><tr><td>2013</td><td>88.4</td></tr><tr><td>2014</td><td>90.0</td></tr><tr><td>2015</td><td>144.8</td></tr><tr><td>2016</td><td>201.3</td></tr><tr><td>2017</td><td>223.8</td></tr></table>							Year	Metric Tons	2012	107	2013	88.4	2014	90.0	2015	144.8	2016	201.3	2017	223.8	2012 Actual	2013 Actual	2014 Actual	2015 Actual	2016 Actual	2017 Actual	2017 Target	2018 Target		
Year	Metric Tons																													
2012	107																													
2013	88.4																													
2014	90.0																													
2015	144.8																													
2016	201.3																													
2017	223.8																													
							107	88.4	90.0	144.8	201.3	223.8	≥100.0	≥200.0																
Removal Rate for Cocaine from Non-Commercial Vessels in Maritime Transit Zone																														
Year-to-Year Trend <table><tr><th>Year</th><th>Removal Rate</th></tr><tr><td>2011</td><td>13.4%</td></tr><tr><td>2012</td><td>15.3%</td></tr><tr><td>2013</td><td>9.5%</td></tr><tr><td>2014</td><td>11.5%</td></tr><tr><td>2015</td><td>7.1%</td></tr><tr><td>2016</td><td>8.2%</td></tr></table>							Year	Removal Rate	2011	13.4%	2012	15.3%	2013	9.5%	2014	11.5%	2015	7.1%	2016	8.2%	2012 Actual	2013 Actual	2014 Actual	2015 Actual	2016 Actual	2017 Actual	2017 Target	2018 Target		
Year	Removal Rate																													
2011	13.4%																													
2012	15.3%																													
2013	9.5%																													
2014	11.5%																													
2015	7.1%																													
2016	8.2%																													
							13.4%	15.3%	9.5%	11.5%	7.1%	8.2%	≥11.5%	≥10.0%																

10.3 Maritime Security

due regard to the requirements of national defense, aids to maritime navigation, ice-breaking facilities, and rescue facilities for the promotion of safety on, under, and over the high seas and waters subject to the jurisdiction of the United States; shall, pursuant to international agreements, develop, establish, maintain, and operate icebreaking facilities on, under, and over waters other than the high seas and waters subject to the jurisdiction of the United States; shall engage in oceanographic research of the high seas and in waters subject to the jurisdiction of the United States; and shall maintain a state of readiness to function as a specialized service in the Navy in time of war, including the fulfillment of Maritime Defense Zone command responsibilities.⁵⁰

In 2004, the Coast Guard established the Maritime Law Enforcement Academy in Charleston, South Carolina. The academy prepares Coast Guard personnel to perform as boarding officers and boarding team members; develops the maritime law enforcement skills of professionals from federal, state, and local agencies, as well as the international community; and provides assistance to law enforcement agencies (Figure 10.35).

The Coast Guard also operates an investigative service (Figure 10.36).

The office concentrates on drugs and other smuggling, illegal immigration activities, and environmental violations. The following charts the competencies and skills expected for the professional investigator.

Receipt, analysis, and disposition of allegations(s)

- Obtain data from complainant or source.
- Document complaint in writing.
- Know prosecutorial or regulatory criteria.
- Identify violations (elements of crime) or administrative standards.



Figure 10.35 Maritime Law Enforcement Academy patch.



Figure 10.36 Seal of the U.S. Coast Guard Investigative Service.

Homeland Security

- Review and identify significant information or potential evidence.
- Determine correct disposition of complaint (criminal, civil, or administrative).
- Open investigation, if appropriate, and coordinate with appropriate authorities (internally/externally).

Assessment, focus, and preparation of investigative plan

- Review available information and evidence.
- Review legal decisions and guidelines.
- Review agency programs, operational policies, and procedures.
- Determine focus and scope of investigation.
- Assess and identify required resources.
- Identify potential witnesses, suspects, relevant documents, and evidence.
- Organize and prioritize investigative activities.
- Prepare initial investigative plan.

Conduct investigation

- Maintain focus and follow investigative plan (revise as necessary).
- Prepare for anticipated investigative activities (interviews, taking statements).
- Apply knowledge of laws and regulations.
- Understand and apply techniques to ensure constitutional rights.
- Project a professional image.
- Use good oral and written communicative skills.
- Know evidentiary rules.
- Collect, analyze, and preserve evidence.
- Use appropriate specialized techniques (search warrants, forensics, consensual monitoring).
- Conduct reviews and data inquiries and promptly document such activities.
- Collect and analyze financial data.
- Assess progress and refocus when necessary.
- Coordinate progress with supervisor (prosecutors or management, as appropriate).
- Maintain appropriate liaison.
- Effectively manage the case and assist personnel and meet planned milestones.
- Obtain IG or grand jury subpoenas and testify before grand jury.

Review, organize, and evaluate investigative findings

- Review and understand the information gathered.
- Organize the information and evidence gathered.
- Correlate data, witnesses, and records.
- Consider internal/external customer needs.

Draft report, validate contents, and submit final report

- Write draft report—ensure accuracy, thoroughness, objectivity, proper format, clarity, and correct grammar.
- Review report to ensure information is correct and complete.
- Consider issues such as confidentiality, the Privacy Act, the Freedom of Information Act, and security classification.

- Include disclosure caveats where appropriate.
- Write final report.
- Distribute to appropriate entities.

Post investigative tasks

- Know rules of criminal and civil procedures.
- Assist with preparation for court/administrative proceedings.
- Serve witness subpoenas.
- Assist U.S. attorney/district attorney at trial.
- Testify at trial.
- Document and report results, dispositions, and outcomes.
- Obtain disposition of exhibits and evidence after trial/hearing.
- Return and document proper disposition of documents and evidence.
- Review the organization of investigative files for efficient retrieval.
- Archive investigative files.
- Ensure information management database reflects accurate and final case information.⁵¹

The Coast Guard tackles law enforcement from the homeland security end too. Here, the Coast Guard displays its multitasking ability and its capacity to blend safety, emergency, defense, and homeland protection into its mission. “Domestically, the Coast Guard–led Area Maritime Security Committees carry out much of the maritime security regimes effort.”⁵²

Counterterrorism efforts are an ongoing Coast Guard responsibility as well, with a plethora of activities including the Maritime Security Response Team (MSRT)—a first responder to terrorist activities on the seas (Figure 10.37).

In the area of homeland security, the Coast Guard assumes these responsibilities:

- Protect ports, the flow of commerce, and the marine transportation system from terrorism.



Figure 10.37 MSRT boat crews maneuver into formation during training on Chesapeake Bay, February 17, 2011. The mission of the MSRT is to provide a short-notice, threat-tailored, maritime response force to deter, protect against, and respond to threats of maritime terrorism and to higher-risk criminal law enforcement threats on the water or in a port. (U.S. Coast Guard photo by Petty Officer 2nd Class Michael Anderson.)

Homeland Security

- Maintain maritime border security against illegal drugs, illegal aliens, firearms, and WMDs.
- Ensure that we can rapidly deploy and resupply our military assets, both by keeping Coast Guard units at a high state of readiness and by keeping marine transportation open for the transit assets and personnel from other branches of the armed forces.
- Protect against illegal fishing and indiscriminate destruction of living marine resources, and prevention and response to oil and hazardous material spills—both accidental and intentional.
- Coordinate efforts and intelligence with federal, state, and local agencies.

The Coast Guard also works closely with the other branches of the military to provide homeland defense and civil support to federal, state, and local agencies in the United States, and includes the increased security measures taken after the 9/11 terrorist attacks.

The Coast Guard joined the other services in making its services available to the larger law enforcement community. This program, dubbed Operation Noble Eagle, seeks to meld the missions of the military into the homeland strategy (Figure 10.38).

Career opportunities abound for those interested in military service with a safety and law enforcement approach. The Coast Guard career track delivers fascinating and challenging paths to professionalism.

10.3.4.3 Cargo and Ports

The responsibility for cargo and port protection resides primarily with the U.S. Coast Guard, though its aligned partners—DHS and the Customs and Immigration Service—aid in the endeavor. See Figure 10.39.⁵³

Bureaucratically, the Coast Guard administers its cargo, container, and facilities program through its Inspection and Compliance Directorate.

For the Coast Guard, as part of its overall mission of safety and security on the high seas and waterways, it would be a natural and very complementary function for this service. With billions of tons of cargo, and nearly 52,000 foreign ships visiting the United States, the job can be daunting.⁵⁴ Balance this with the entrepreneurial bent of the shipping and cargo industry—which needs to move goods and services fast, efficiently, and profitably—and you have a delicate policy problem. On the one hand, safety and security issues run front and center, yet on the other hand, the Coast Guard needs to be sensitive to the question of productivity and finance. Some have argued that the costs of maritime security may be too high and not worth the investment.⁵⁵ From afar, the costs associated with ensuring security are staggering and sometimes demonstrate the subservience of the maritime industry, which is “at the beck and call of a government whose legal initiatives, understandably, are more in tune with security than economy.”⁵⁶ In a global



Figure 10.38 Operation Noble Eagle patch.

DHS Science and Technology Directorate Air Cargo Screening Program

Air Cargo Screening and the evolving threat

In the United States, nearly all domestic commercial passenger flights carry air cargo. Air cargo makes up about 50% of the goods carried in passenger aircraft. Without effective screening of air cargo, passenger safety could be compromised. In 2007, Public Law 110-53 “Implementing Recommendations of the 9/11 Commission Act,” mandated all cargo on passenger aircraft must be 100% screened for explosive and other threat devices, to at least checked baggage standards, before loading on passenger aircraft. To meet this mandate, TSA created the Certified Cargo Screening Program in which they certify private companies to screen air cargo using TSA approved screening equipment. Air cargo screening is an important part of the Aviation Security Screening Triad (see below) requiring new technologies to address evolving threats and maintain screening effectiveness.



Air cargo is a key part of the Aviation Security Screening Triad. Air Cargo Screening is carried out through private companies (not TSA).

The S&T Air Cargo Screening Program fulfills a vital part of S&T’s mission to provide Aviation Security R&D to support the Transportation Security Administration’s air cargo screening security mission.

Given the great variety of air cargo commodity types, achieving effective air cargo screening is a daunting task. The Air Cargo Screening Program addresses these challenges by developing new security technologies to enhance current operational air cargo screening capabilities, so that diverse and complex cargo can be effectively screened in a cost efficient manner. This broad, ongoing effort seeks to address the current and evolving air cargo security needs of our stakeholders (TSA, commercial air carriers, freight forwarders, etc.).



Complex and challenging air cargo commodity types include pallets of heavy industrial parts (electric motors (left)) and skids of consolidated homogenous parcels.

S&T develops advanced technology for improved detection and screening

The Air Cargo Screening Program is investing in a portfolio of next generation products for the cost effective screening of air cargo. This includes technologies to develop low cost computed tomography (CT) or CT-like systems for screening whole skids, advanced trace detection systems such as high sensitivity portable trace detectors, intelligent “Operator Assist” software tools to assist the operator in effective screening of complex commodities, and standardized graphical user interfaces to improve operator proficiency and ease the burden of training operators. Air cargo screening equipment is purchased by certified private screening companies, not by the TSA. The cost of air cargo screening equipment is important to the screening companies; hence, it is an important consideration in our development efforts.

S&T Customers/Partners

Though TSA is the primary stakeholder for S&T’s Air Cargo Screening Program, our integrated product team includes members from other DHS components. Our research and development partners include the Transportation Security Laboratory, national laboratories, universities, and the air cargo private sector.



**Homeland
Security**
Science and Technology

To learn more about EXD’s Air Cargo Program, contact
SandT.Explosives@hq.dhs.gov

2016 09 26

Figure 10.39 DHS S&T Directorate air cargo screening program.

economy, with significant trade entering American ports each and every day, the imposition of security measures in a free economy requires keen balancing. Implementing “new security policies with economic and trade objective is a complicated task given the potential risks to human life should the United States under-protect its borders.”⁵⁷



Figure 10.40 Logo for the Coast Guards Office of Port and Facility Compliance.

Each and every day, the U.S. Coast Guard is responsible for every visitation of a foreign ship, the safety and security of America's ports, and the implementation of sweeping maritime policies.⁵⁸

The Coast Guard's Office of Port and Facility Compliance (Figure 10.40) is responsible for

- Overseeing onshore and offshore domestic commercial facilities, including deep-water ports, and cargo safety, security, and environmental protection compliance programs, including the direction of Coast Guard field activities, and industry partnerships in support of applicable laws and regulations
- Advising the Office of Investigation and Analysis regarding the notice of violation enforcement program policy as applied to cargo and commercial facilities
- Maintaining liaison and outreach with key industry, interagency, and international partners on related facility and cargo safety, security, and environmental protection activities
- Developing policy for facility security plans (FSPs) review and approval, facility alternative security programs (ASPS), and public access/waivers/exemptions
- Establishing and interpreting standards and regulations, and participating in the rule making and the legislative change process for onshore and offshore domestic commercial facilities
- Administering the standard safety and security Facility Inspection and Pollution Prevention Compliance programs
- Administering program activities for military and commercial explosives, radioactive materials, packaged hazardous materials, cargoes of particular hazard, and classified cargoes
- Maintaining a database of all U.S. waste reception
- Developing inspection, enforcement, and safety and security policy for the Coast Guard Container Inspection Program and overseeing the operation of the Container Inspection Training and Assist Team (CITAT)
- Developing regulations and policy guidance for the implementation of a biometric credential for port workers and updating access control regulations and security plan requirements to implement requirements for such a credential
- Establishing policy and policy guidance and overseeing the enforcement of international treaties, conventions, and domestic regulations for domestic onshore and off-shore commercial facilities, including deep-water ports and cargoes.

- Coordinating with interdepartmental agencies and other departments on the application of a coordinated cargo safety and security legislations, regulations, standards, and rules
- Coordinating U.S. participation in international maritime groups

10.3.4.3.1 Operation Homeport

Homeport is the code name given by the Coast Guard to signify all of its port activities. The activities are extensive, and this short section will only highlight a few of them (Figure 10.41).

Internet Exercise: To become familiar with the diverse Homeport functions, visit <https://homeport.uscg.mil/>.

10.3.4.3.1.1 Port and Harbor Facilities

Port facilities are subject to a wide array of safety and security standards. Coast Guard personnel inspect the facilities—some 3,200 facilities in the United States alone. Each facility is required under the Maritime Security Act of 2002 to develop and implement a security plan. By 2005, some 9,500 vessels and 3,500 facilities submitted both a security assessment and a security plan. The Coast Guard was entrusted with assessing these plans and, once determining vulnerabilities, working with these parties to adjust and correct deficiencies. Coast Guard inspectors enter the facility to determine the consistency of the plan with the reality of that facility. Breaches in facilities are noted as well as deficiencies relating to record keeping and access control.

Internet Exercise: For the federal regulations regarding the content of the security plan, see http://edocket.access.gpo.gov/cfr_2003/julqtr/pdf/33cfr105.305.pdf.

By 2006, the GAO, when reviewing the results of Coast Guard inspections, found patterns of deficiencies.⁵⁹ See Figure 10.42 for a chart depicting the results.

Upon the completed inspection, the Coast Guard issues a vulnerability report that the carrier will concur with or appeal (Figure 10.43).⁶⁰

10.3.4.3.1.2 Container Inspection

The Coast Guard deploys teams to moving and stationary vessels for inspection of cargo and containers. The Coast Guard has developed and deployed CITATs to conduct container inspections at harbors and ports.



Figure 10.41 Operation Homeport inspection.

Homeland Security

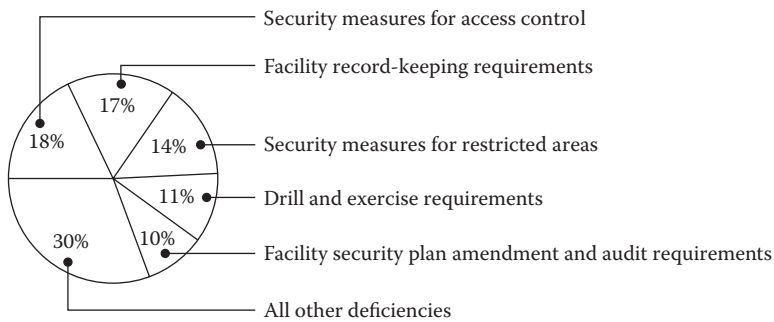


Figure 10.42 Types of deficiencies noted by the Coast Guard in facility inspections during 2006.

10.3.4.3.1.3 Vessel Inspection

On the high seas and waterways, the Coast Guard has jurisdictional authority to board vessels for inspection purposes. This practice is one of its most crucial missions. Section 89 of Title 14 of the U.S. Code authorizes the Coast Guard to board vessels subject to the jurisdiction of the United States, any time on the high seas and on waters over which the United States has jurisdiction, to make inquiries, examinations, inspections, searches, seizures, and arrests. Even despite the statutory authority, there are multiple reasons why boarding programs exist.

First, the Coast Guard tracks and issues certificates of operation to vessel owners.

Second, the Coast Guard maintains a central depository of vessel records at its National Vessel Documentation Center. Records of registered vessels are fully cataloged and documented and serve as an information center in the event of accident or other calamity.

Third, the Coast Guard boards ships to conduct inspections or to carry out interdiction or intervention actions in the event of criminal activities. In the first instance, the Coast Guard may simply board under a voluntary request for ship inspection (Figure 10.44).

To commence the voluntary inspection program, the applicant needs only fill out the request as outlined in Figures 10.45 or 10.46.

In the latter instance (involuntary boarding), the Coast Guard may board if legally justified. Any question regarding safety, any issue of equipment, and surely any suspicion of illegal activity make boarding, despite a lack of consent, acceptable. When compared with their civilian law enforcement counterparts, whose action generally must be supported by probable cause, the rationale for boarding is much less legally rigorous. The Coast Guard expends considerable energy preparing boarding officers and, just as attentively, refines the boarding process to ensure a professional and legally defensible protocol. The Coast Guard certifies boarding officers in training locales at its network of facilities. The designated curriculum for the boarding officer stresses a legalistic approach to training, as evidenced by the subject matter.

- Authority and jurisdiction
- Use of force
- Tactical procedures
- Criminal law
- Constitutional law
- Defensive tactics
- Arrest procedures
- Maritime law enforcement boarding procedures

10.3 Maritime Security

DEPARTMENT OF HOMELAND SECURITY U.S. Coast Guard FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY		OMB No: 1625-0077 Exp. Date: 11/30/2022																																
An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The Coast Guard estimates that the average burden for this report is 60 minutes. You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to: Commandant (CG-FAC), U.S. Coast Guard Stop 7501, 2703 Martin Luther King Jr Ave SE, Washington, DC 20593-7501 or Office of Management and Budget, Paperwork Reduction Project (1625-0077), Washington, DC 20503.																																		
FACILITY IDENTIFICATION																																		
1. Name of Facility		Date:																																
2. Address of Facility	3. Latitude																																	
	4. Longitude																																	
	5. River Name (if applicable)																																	
	6. River Mile (if applicable)																																	
	7. Captain of the Port Zone																																	
8. Type of Operation (check all that apply) <table style="width: 100%; border: none;"> <tr> <td>☐ Barge Fleeting</td> <td>☐ Bulk Oil (PETROLEUM) Refinery</td> <td>☐ CDC* – Other</td> <td>☐ Passengers (Other)</td> </tr> <tr> <td>☐ Break Bulk (HAZMAT)</td> <td>☐ CDC* – Ammonia, Anhydrous</td> <td>☐ Chemical Production</td> <td>☐ Radioactive Material – Class 7</td> </tr> <tr> <td>☐ Break Bulk (non-HAZMAT)</td> <td>☐ CDC* – Chlorine</td> <td>☐ Container</td> <td>☐ Ro-Ro</td> </tr> <tr> <td>☐ Bulk Dry (HAZMAT)</td> <td>☐ CDC* – LNG</td> <td>☐ Explosives</td> <td>☐ If other, explain below:</td> </tr> <tr> <td>☐ Bulk Dry (non-HAZMAT)</td> <td>☐ CDC* – LPG</td> <td>☐ Military Supply</td> <td></td> </tr> <tr> <td>☐ Bulk Liquid (HAZMAT)</td> <td>☐ CDC* – other LHGs</td> <td>☐ Offshore Support</td> <td></td> </tr> <tr> <td>☐ Bulk Liquid (non-HAZMAT)</td> <td>☐ CDC* – Material Poisonous by Inhalation (PIH-TIH)</td> <td>☐ Passengers (Cruise)</td> <td></td> </tr> <tr> <td>☐ Bulk Oil (PETROLEUM) Storage/Transfer</td> <td></td> <td>☐ Passengers (Ferry)</td> <td></td> </tr> </table> * Certain Dangerous Cargo			☐ Barge Fleeting	☐ Bulk Oil (PETROLEUM) Refinery	☐ CDC* – Other	☐ Passengers (Other)	☐ Break Bulk (HAZMAT)	☐ CDC* – Ammonia, Anhydrous	☐ Chemical Production	☐ Radioactive Material – Class 7	☐ Break Bulk (non-HAZMAT)	☐ CDC* – Chlorine	☐ Container	☐ Ro-Ro	☐ Bulk Dry (HAZMAT)	☐ CDC* – LNG	☐ Explosives	☐ If other, explain below:	☐ Bulk Dry (non-HAZMAT)	☐ CDC* – LPG	☐ Military Supply		☐ Bulk Liquid (HAZMAT)	☐ CDC* – other LHGs	☐ Offshore Support		☐ Bulk Liquid (non-HAZMAT)	☐ CDC* – Material Poisonous by Inhalation (PIH-TIH)	☐ Passengers (Cruise)		☐ Bulk Oil (PETROLEUM) Storage/Transfer		☐ Passengers (Ferry)	
☐ Barge Fleeting	☐ Bulk Oil (PETROLEUM) Refinery	☐ CDC* – Other	☐ Passengers (Other)																															
☐ Break Bulk (HAZMAT)	☐ CDC* – Ammonia, Anhydrous	☐ Chemical Production	☐ Radioactive Material – Class 7																															
☐ Break Bulk (non-HAZMAT)	☐ CDC* – Chlorine	☐ Container	☐ Ro-Ro																															
☐ Bulk Dry (HAZMAT)	☐ CDC* – LNG	☐ Explosives	☐ If other, explain below:																															
☐ Bulk Dry (non-HAZMAT)	☐ CDC* – LPG	☐ Military Supply																																
☐ Bulk Liquid (HAZMAT)	☐ CDC* – other LHGs	☐ Offshore Support																																
☐ Bulk Liquid (non-HAZMAT)	☐ CDC* – Material Poisonous by Inhalation (PIH-TIH)	☐ Passengers (Cruise)																																
☐ Bulk Oil (PETROLEUM) Storage/Transfer		☐ Passengers (Ferry)																																
VULNERABILITY AND SECURITY MEASURES #1																																		
9a. Vulnerability		9b. Vulnerability Category ☐ If other, explain																																
10a. Selected Security Measures (MARSEC Level 1)		10b. Security Measures Category ☐ If other, explain																																
11a. Selected Security Measures (MARSEC Level 2)		11b. Security Measures Category ☐ If other, explain																																
12a. Selected Security Measures (MARSEC Level 3)		12b. Security Measures Category ☐ If other, explain																																
VULNERABILITY AND SECURITY MEASURES #2 (if applicable)																																		
9a. Vulnerability		9b. Vulnerability Category ☐ If other, explain																																
10a. Selected Security Measures (MARSEC Level 1)		10b. Security Measures Category ☐ If other, explain																																
11a. Selected Security Measures (MARSEC Level 2)		11b. Security Measures Category ☐ If other, explain																																
12a. Selected Security Measures (MARSEC Level 3)		12b. Security Measures Category ☐ If other, explain																																

CG-6025 (11/19)

Page 1 of 3

Figure 10.43 Facility vulnerability and security measures summary form. (From U.S. Department of Homeland Security.)

(Continued)

INSTRUCTIONS FOR CG-6025: FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY																																															
This form satisfies the requirements for Facility Vulnerability and Security Measures Summary submission found in the Code of Federal Regulations for Facility Security. Form CG-6025A, Vulnerability and Security Measures Addendum, may be used as a continuation of form CG-6025, in order to submit additional vulnerabilities and security measures. If a facility owner or operator submits Facility Vulnerability and Security Measures Summary pertaining to more than one facility, form CG-6025, shall be submitted to document each additional facility. Each owner or operator that submits one Facility Security Plan (FSP) to cover two or more facilities of similar design and operation must address facility-specific information that includes the design and operational characteristics of each facility and must complete a separate CG-6025 form for each facility covered by the plan (33 CFR § 105.410(f)).																																															
BLOCK 1	Self-Explanatory.	BLOCK 8a	Enter a concise description of a selected security measure identified in the plan for MARSEC Level 1 that will mitigate the vulnerability you addressed.																																												
BLOCK 2	Street Address.	BLOCK 8b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.																																												
BLOCK 3	If available, provide latitude to nearest tenth of a minute.	BLOCK 9a	Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 2 that will mitigate the vulnerability you addressed.																																												
BLOCK 4	If available, provide longitude to nearest tenth of a minute.	BLOCK 9b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.																																												
BLOCK 5	Provide the Captain of the Port Zone from the list below in which your facility resides. Their respective zones are described in 33 CFR Part 3.	BLOCK 10a	Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 3 that will mitigate the vulnerability you addressed.																																												
BLOCK 6	Check all applicable operations that are conducted at your facility. For example, a container terminal would most likely need to indicate the following types of operation: CDC - Ammonia, Anhydrous; CDC - Chlorine; CDC - Material Poisonous by Inhalation (PIH-TIH); CDC -Other; Container; Explosives; Radioactive Material - Class 7; and Ro-Ro. If you select other, please explain in the box provided.	BLOCK 10b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.																																												
BLOCK 7a	Enter a concise description of a vulnerability identified in your facility's assessment. Provide location information if appropriate.																																														
BLOCK 7b	Enter the vulnerability identification code from the KEY to categorically identify the vulnerability you described. More than one category may be used. If you select other, please explain in the box provided.																																														
CAPTAIN OF THE PORT ZONE: <table border="0"> <tbody> <tr> <td>Boston</td> <td>Houma</td> <td>New Orleans</td> <td>San Juan</td> </tr> <tr> <td>Buffalo</td> <td>Houston-Galveston</td> <td>New York</td> <td>Sault St. Marie</td> </tr> <tr> <td>Charleston</td> <td>Jacksonville</td> <td>North Carolina</td> <td>Savannah</td> </tr> <tr> <td>Columbia River</td> <td>Key West</td> <td>Northern New England</td> <td>Southeast Alaska</td> </tr> <tr> <td>Corpus Christi</td> <td>Lake Michigan</td> <td>Ohio Valley</td> <td>Southeastern New England</td> </tr> <tr> <td>Delaware Bay</td> <td>Long Island Sound</td> <td>Pittsburgh</td> <td>St. Petersburg</td> </tr> <tr> <td>Detroit</td> <td>Los Angeles-Long Beach</td> <td>Port Arthur</td> <td>Upper Mississippi River</td> </tr> <tr> <td>Duluth</td> <td>Lower Mississippi River</td> <td>Prince William Sound</td> <td>Western Alaska</td> </tr> <tr> <td>Guam</td> <td>Maryland-NCR</td> <td>Puget Sound</td> <td></td> </tr> <tr> <td>Hampton Roads</td> <td>Miami</td> <td>San Diego</td> <td></td> </tr> <tr> <td>Honolulu</td> <td>Mobile</td> <td>San Francisco Bay</td> <td></td> </tr> </tbody> </table>				Boston	Houma	New Orleans	San Juan	Buffalo	Houston-Galveston	New York	Sault St. Marie	Charleston	Jacksonville	North Carolina	Savannah	Columbia River	Key West	Northern New England	Southeast Alaska	Corpus Christi	Lake Michigan	Ohio Valley	Southeastern New England	Delaware Bay	Long Island Sound	Pittsburgh	St. Petersburg	Detroit	Los Angeles-Long Beach	Port Arthur	Upper Mississippi River	Duluth	Lower Mississippi River	Prince William Sound	Western Alaska	Guam	Maryland-NCR	Puget Sound		Hampton Roads	Miami	San Diego		Honolulu	Mobile	San Francisco Bay	
Boston	Houma	New Orleans	San Juan																																												
Buffalo	Houston-Galveston	New York	Sault St. Marie																																												
Charleston	Jacksonville	North Carolina	Savannah																																												
Columbia River	Key West	Northern New England	Southeast Alaska																																												
Corpus Christi	Lake Michigan	Ohio Valley	Southeastern New England																																												
Delaware Bay	Long Island Sound	Pittsburgh	St. Petersburg																																												
Detroit	Los Angeles-Long Beach	Port Arthur	Upper Mississippi River																																												
Duluth	Lower Mississippi River	Prince William Sound	Western Alaska																																												
Guam	Maryland-NCR	Puget Sound																																													
Hampton Roads	Miami	San Diego																																													
Honolulu	Mobile	San Francisco Bay																																													

Figure 10.43 (*CONTINUED*) Facility vulnerability and security measures summary form. (From U.S. Department of Homeland Security.)

(Continued)

KEY			
<u>VULNERABILITY CATEGORIES</u>			
Physical Security	PHS	That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against terrorism, espionage, sabotage, damage, and theft.	
Structural Integrity	STI	The design and material construction characteristics of piers, facilities, and associated structures.	
Transportation Infrastructure	TRI	Infrastructure that may be exploited during an attack, other than utilities.	
Utilities	UTI	The essential equipment and services that are vital to the operation of the facility.	
Radio & Telecommunications	RAT	That part of security concerned with measures to protect radio and telecommunication equipment, including computer systems and networks (also known as Cyber security).	
Personnel Protection Systems	PPS	Equipment, Gear, or Systems designed to protect facility personnel (i.e. weapons, body armor).	
Procedural Policies	PRP	Plans, Policies, and Procedures for specific operations.	
Coordination and Information Sharing	CIS	The ability to coordinate and receive/share information with local/state/federal agencies and other commercial entities.	
Preparedness	PRE	Implementation of Plans, Policies, and Procedures through Training, Drills, and Exercises conducted to improve security awareness, prevention, and response.	
<u>SECURITY MEASURES</u>			
Access Control	ACC	Lighting	LIT
Barriers	BAR	Other	OTH
Cargo Control	CAC	Patrols	PAT
Communications	COM	Planning, Policies, & Procedures	PPP
Coordination	COR	Redundancy	RED
Credentialing	CRE	Response	RES
Detection	DET	Stand-off Distance	SOD
Guard Force	GUF	Structural Hardening	STH
IT Security	ITS	Surveillance	SUR
Inspections	INS	Training	TRA
Intelligence	INT	Vessels/Vehicles	VEV

Figure 10.43 (*CONTINUED*) Facility vulnerability and security measures summary form. (From U.S. Department of Homeland Security.)



Figure 10.44 Coast Guard officers conducting inspections.

- PWCS (ports, waterways, and coastal security) boarding procedures
- Confined spaces
- Boating safety regulations
- Commercial fishing industry regulations
- Boating under the influence enforcement
- Testify in court
- Hostage situations
- Fraudulent document

The Coast Guard lays out a precise protocol for boarding a vessel. A uniformed Coast Guard boarding team gives notification of its intent to board. Generally, the team is armed. At first, the team will conduct an initial safety inspection to identify any obvious safety hazards and to ensure the sea worthiness of the vessel. The boarding officer will then ask to see the vessel registration or documentation and proceed with the inspection. The scope of the vessel inspection during most boardings is limited to determining the vessel's regulatory status (e.g., commercial, recreational, passenger, cargo, or fishing vessel) and checking for compliance with U.S. civil law applicable to vessels of that status. The Coast Guard may also enforce U.S. criminal law. The boarding officer then completes a Coast Guard boarding form and notes any discrepancies (Figure 10.47).

Space limitations make impossible a full picture of how the U.S. Coast Guard lends its services in the maritime world. In many ways, it is the branch of the service most dedicated to the cause of homeland security. Every minute of its operations is about safety and security, and since 9/11, the Coast Guard has been called on to do more than it has ever imagined since its inception in 1790. Of all the governmental entities called on to strike back and detect our enemies, the Coast Guard has been asked to reinvent itself. A report about the Coast Guard from the Government Accountability Office warned of this tendency to throw everything at this arm of the service.

The difficulty of meeting these challenges is compounded because the Coast Guard is not just moving to a new parent agency: it is also substantially reinventing itself because of its new

10.3 Maritime Security

U.S. DEPARTMENT OF HOMELAND SECURITY U.S. COAST GUARD CG-3752 (Rev. 6-04)	APPLICATION FOR INSPECTION OF U.S. VESSEL	FORM APPROVED OMB NO: 1625-0002 Expiration Date: 06/30/2017
An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The Coast Guard estimates that the average burden for this report is 15 mins. You may submit any comments concerning the accuracy of this burden estimate or any suggestion reducing the burden to: Commandant (G-MOC), U.S. Coast Guard, Washington, DC 20593-0001 or Office of Management and Budget, Paperwork Reduction Project (1625-0002), Washington, DC 20503.		
TO: Officer in Charge, Marine Inspection Marine Inspection Zone _____ The undersigned applies to have the ☐ Steam Vessel ☐ Motor Vessel ☐ Motorboat ☐ Barge ☐ Other (Indicate) _____		Address to reply to: TELEPHONE NUMBER: DATE:
named _____ Official or Award No. _____ inspected under the laws of the United States; to be employed as a ☐ Passenger Vessel (No. of Passengers _____) ☐ Cargo Vessel ☐ Tank Vessel ☐ MODU ☐ Other (Indicate) _____ on the following route: (Waters, Geographical limits) _____ _____ Liquid cargo in bulk ☐ will ☐ will not be carried as follows: ☐ Flammable or Combustible (Indicate grade) _____ ☐ Chemicals (Indicate) _____ Length of vessel _____ ft. Hull material: ☐ Steel ☐ Other (Indicate) _____ Vessel will be at (Port, Pier, etc.) _____ The current Certificate of Inspection expires on _____ . Inspection is desired on _____ . Cargo Ship Safety Construction Certificate to be issued by ☐ ABS ☐ USCG. Vessel ☐ is ☐ is not to be classed. If classed, indicate Classification Society: ☐ ABS ☐ Other (Indicate) _____ I CERTIFY that previous application for this inspection ☐ has ☐ has not been made. I further certify that I have instructed the master to present the vessel ready in all respects for the above requested inspection on the date specified. I understand that if this inspection is to be conducted at foreign port or place the vessel owners will be billed for the costs incurred in accordance with 46 USC 385b-1. (Signature) _____ (Title) _____		

PREVIOUS EDITION IS OBSOLETE

Figure 10.45 Application for inspection of a U.S. vessel by the Coast Guard.

security role. Basically, the agency faces a fundamental tension in balancing its many missions. It must still do the work it has been doing for years in such areas as fisheries management and search and rescue, but now its resources are deployed as well in homeland security and even in the military buildup in the Middle East. The Coast Guard's expanded role in homeland security,

Homeland Security

U.S. DEPARTMENT OF HOMELAND SECURITY U.S. COAST GUARD CG-3752A Rev. (01-07)	APPLICATION FOR INSPECTION OF U.S. VESSEL (NEW CONSTRUCTION)	FORM APPROVED OMB NO: 1625-0002 Exp Date: 06/30/2017
An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The Coast Guard estimates that the average burden for this report is 15 mins. You may submit any comments concerning the accuracy of this burden estimate or any suggestion reducing the burden to: Commandant (CG-3PCV), U.S. Coast Guard, Washington DC 20593-0001 or Office of Management and Budget, Paperwork Reduction Project (1625-0002), Washington, DC 20503.		
TO: Officer in Charge, Marine Inspection		
The undersigned applies for inspection of the new vessel:		
_____ <i>(Name-if known)</i> _____ <i>(Hull Number)</i>		
Multi Service Requested? <i>(Check one)</i> ☐ Yes ☐ No _____ <i>(Service: Passenger/Cargo/OSV/etc.)</i>		
Route: _____ Intended Hailing Port: _____		
Inspected under the provisions of 46 CFR Subchapter(s) (D/I/K/L/T, etc.): _____		
At (Shipbuilder): _____		
Point of Contact at Builder's Yard: _____		
Address/Phone: _____		
Contract Date: _____ Keel Laid Date: _____		
Est. Date Construction Begins: _____ Est. Delivery Date: _____		
Length: _____ Breadth: _____ Depth: _____		
Estimated Tonnage: Regulatory Gross: _____ Net: _____		
International Gross: _____ Net: _____		
Hull Material: _____ Propulsion Type: _____		
No. of Engines: _____ HP of Each: _____ No. of Shafts: _____		
Propulsion Automation for Machinery Space <i>(Check one)</i> ☐ Yes ☐ No		
Vessel to be Classed <i>(Check one)</i> ☐ Yes ☐ No By (Class Society) _____		
If Yes, is inspection under the provisions of NVIC 10-82 requested? <i>(Check one)</i> ☐ Yes ☐ No <i>(A complete list of NVIC's can be viewed at www.uscg.mil/hq/g-m/nvic/)</i>		
International Certificates (SOLAS, MARPOL, etc.) requested <i>(Check one)</i> ☐ Yes ☐ No		

U.S. DEPT. OF HOMELAND SECURITY, USCG, CG-3752A (Rev. 01-07)

Figure 10.46 Application for inspection of a U.S. vessel by the Coast Guard (New construction).
(Continued)

Proposed Manning: _____ Industrial/ Scientific _____ Offshore Workers _____ Persons in Addition to Crew _____ Vessel Owner: _____ Address: _____ Point of Contact & Phone: _____	Requested Number of: Passengers _____
<u>SHIPYARD OR DESIGN AGENT SUBMITTING DRAWINGS FOR APPROVAL</u>	
Name: _____ Address: _____ Point of Contact & Phone: _____ New Hull Design Type (Check one) ☐ Yes ☐ No If Sistered, Parent Hull is _____ built at _____ (Name/Official #)	
<u>TYPES OF CARGO TO BE CARRIED</u>	
Oil Cargos? (Check one) ☐ Yes ☐ No If yes, describe here or attach separate sheet that lists each intended cargo, grade, and quantity. Please include all NLS Cargos and quantities as well.	
Chemical Cargos? (Circle one) ☐ Yes ☐ No If yes, describe here or attach separate sheet that lists each intended cargo and quantity.	
Deck Cargo? (Circle one) ☐ Yes ☐ No If yes, amount _____ (in Long Tons)	
Person Submitting Application: _____ Title: _____ Signature: _____ Date: _____	
At this stage of your new construction project we realize you may not possess the information to complete every section on this form. However, a fully completed form will allow us to better facilitate the inspection of your new vessel.	

Figure 10.46 (CONTINUED) Application for inspection of a U.S. vessel by the Coast Guard (New construction).



Figure 10.47 Coast Guard boarding a vessel for inspection.

along with its relocation in a new agency, has changed many of its working parameters, and its adjustment to this role remains a work in process. Much work remains.⁶¹

If history demonstrates anything, it would be the capacity of the Coast Guard to meet any challenge assigned to it. The Coast Guard adapts to meet the mission of homeland protection and makes a mighty contribution in the fight against terrorism.

10.4 Rail and Mass Transit

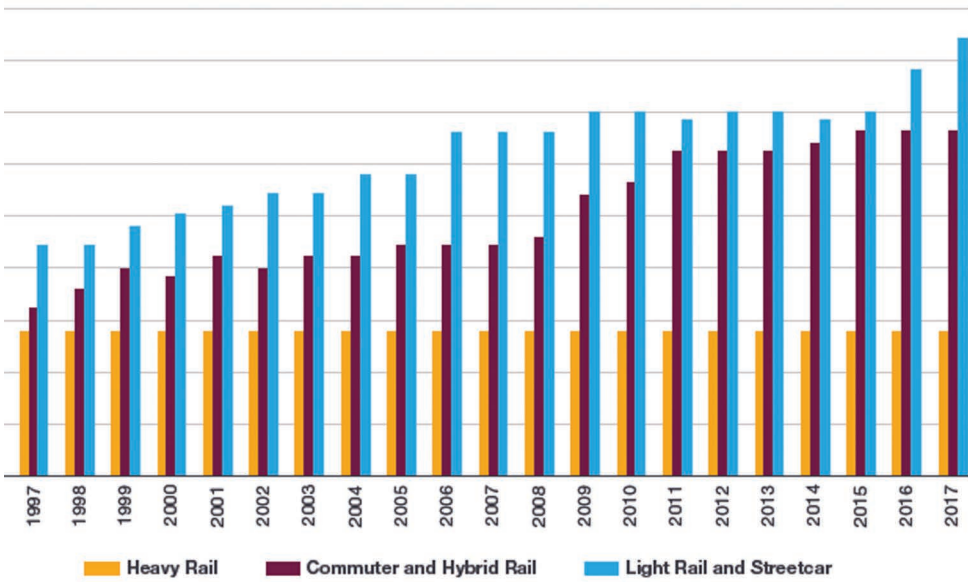
The task of securing the country's rail and mass transit system is just as critical as the air industry protections. Mass transit systems carry nearly ten billion passengers per year and the mass transportation fleet is nearly 150,000 vehicles, and the trend toward mass transit is both short term and longitudinally upward (Figure 10.48).⁶²

Amtrak carries nearly 31 million passengers on its national network.⁶³ The country's rail system, a series of weaving lines for both freight and passenger traffic, constitutes a major part of this country's economic life. In the world of commerce, trains deliver more cargo per mile, and more efficiently than any on-land trucking company is capable of doing. "Every day, more than one million shipments of hazardous chemicals are transported throughout the nation's infrastructure; a large percentage of these chemicals are transported by rail and are prone to becoming airborne."⁶⁴ Since 2004, transit use has grown more than population or highway travel.⁶⁵

The security of this commercial flow is critical to the economic health of the United States, and just the sort of target a terrorist would hope to disrupt. If terrorists seek to inflict widespread harm on the U.S. economy, they have "a number of strategies that pose serious threats to and through the rail system of the country"⁶⁶ (Figure 10.49).

The potential for both human and infrastructural destruction is easy to project and anticipate. For the terrorist, the prime aim generally relates to larger, more grandiose impacts. The act may "use the rails as a way of conveying an instrument of mass destruction on its human agents than an attack on any one point in the physical infrastructure."⁶⁷ As a result, the target of mass transit and its infrastructure is attractive due to the strength of its destructive message. A horrid picture of destruction and loss of life occurred in Madrid, Spain, in 2004. Two hundred people lost their lives in this terrorist act (Figure 10.50).⁶⁸ In 2005, the London transit bombing is still a searing reality for so many of its victims. Here too the jihadis looked for maximum impact,

30 Years Ago



Segment Line or Route Name	Line Segment Miles	Number of Added Stations	Date Opened	Project Type
2nd Avenue Subway Phase 1	2	4	1/1/17	Extension
The Vine	6.7	34	1/8/17	New System
Green Line East End	0	2	1/11/17	Extension
R Line	10.5	8	2/24/17	Extension
Warm Springs Extension	5.4	1	3/25/17	Extension
QLINE / M-1 Rail	3.3	12	5/12/17	New System
SMART	43	10	8/25/17	New System
EMX West Eugene	4.4	15	9/17/17	Extension
ART	4	5	11/25/17	New System

Figure 10.48 Illustrating the upward trends and increased growth of mass transit systems.



Figure 10.49 High-speed passenger train.

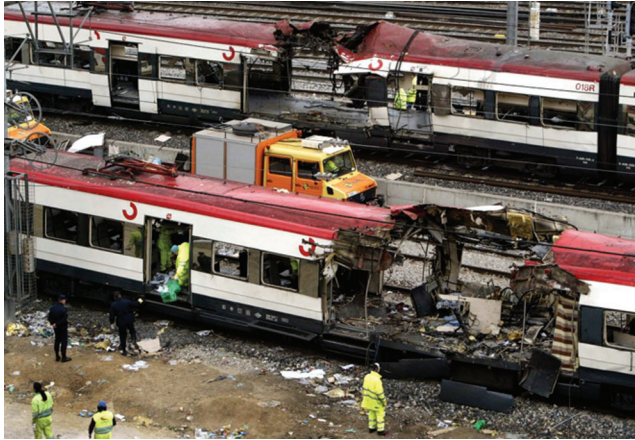


Figure 10.50 Destroyed railway carriages sit on the tracks after the attack on Atocha railway station in Madrid.

where concentrations of people in crowded transit systems delivered the harm and terror sought. Londoners recently memorialized the tenth anniversary of this dreadful event (Figure 10.51).

It is extremely logical to conclude that either passenger or freight might be the means of transport, and if the human casualties are the end sought, the terrorist act may predictably occur near an urban center. In the final analysis, both rail and mass transit systems are part of the family of critical infrastructure essential to a secure America. DHS has now rightfully concluded that mass transit systems and rail lines may be the next generation of threat targets.

The picture of growth in public transportation is simply undeniable (Figure 10.52).⁶⁹

Manifests all the upward trendlines in public transportation.

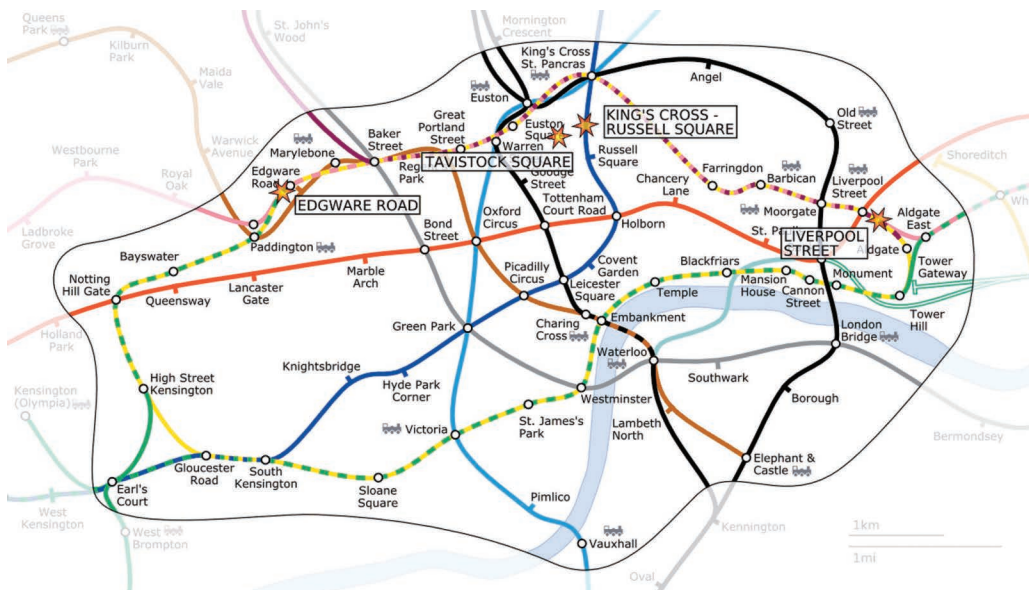


Figure 10.51 The locations of the London bombings of July 7, 2005. (Retrieved from Wikimedia Commons and used per CC 3.0, from user: Ed g2s.)

In rail and mass transit, the demands of risk assessment are more global and less contained than the security checkpoint at an airport. TSA, working closely with state, federal, and local law enforcement, must see vulnerability, threat, and risk in a much larger framework. Instead of the targeted emphasis of passengers at a point of entry, the risk analysis in transit and rail must be conducted at various headquarters and stations, as well as in the whole field of operation.

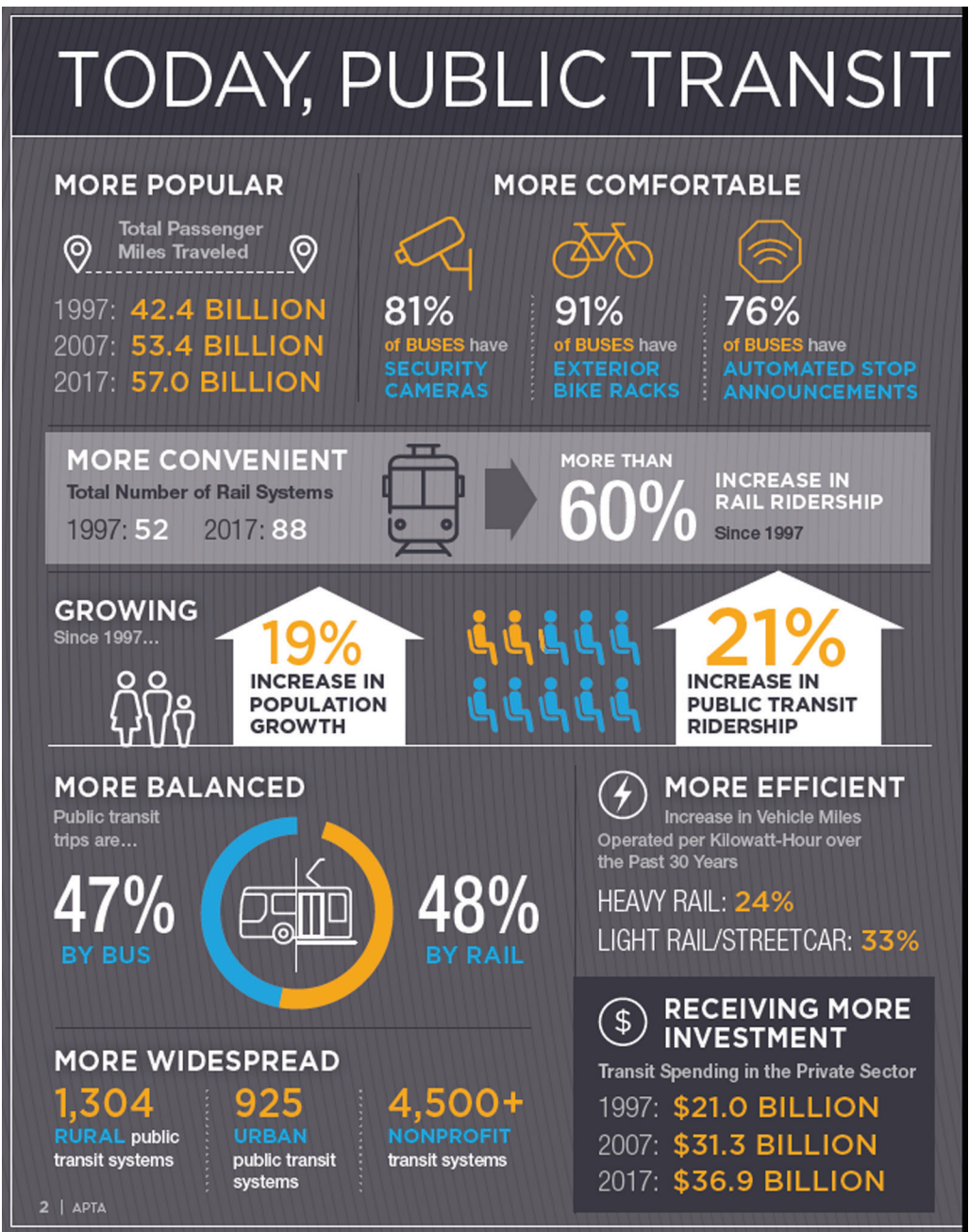


Figure 10.52 Current statistics on public transit in the United States.

(Continued)

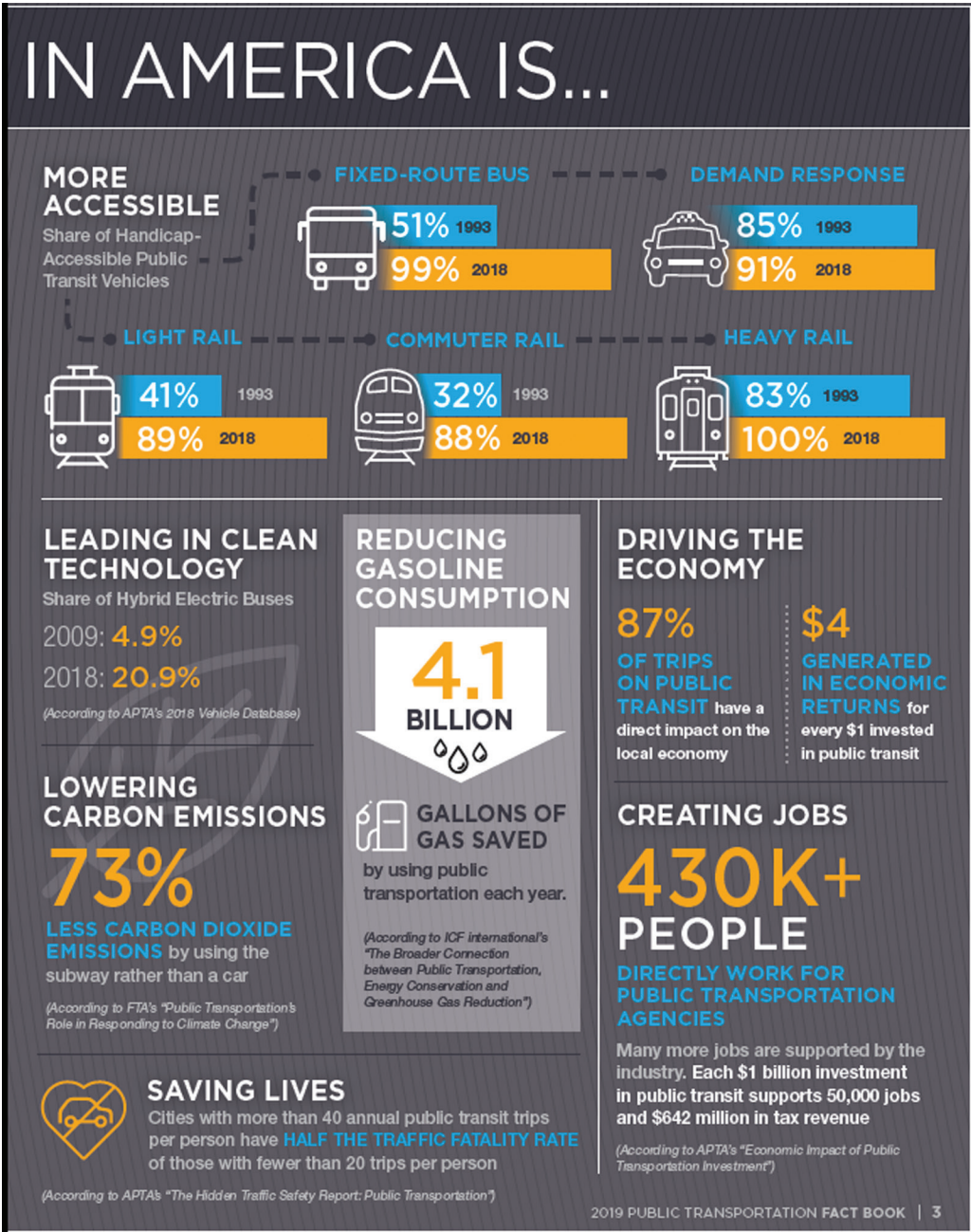


Figure 10.52 (CONTINUED) Current statistics on public transit in the United States.

The tracks are the path to follow, so to speak. In 2010, TSA published a series of recommendations about rail and mass transit, all of which are worthy of our consideration.

1. Designate a lead agency to coordinate periodic modal and cross-modal security risk analyses.
2. Implement an integrated federal approach that consolidates capabilities in a unified effort for security assessments, audits, and inspections to produce more thorough evaluations and effective follow-up actions to reduce risk, enhance security, and reduce burdens on assessed surface transportation entities.
3. Identify appropriate methodologies to evaluate and rank surface transportation systems and infrastructure that are critical to the nation.
4. Implement a multiyear, multiphase grants program based on a long-term strategy for surface transportation security.
5. Establish a measurable evaluation system to determine the effectiveness of surface transportation security grants.
6. Establish an interagency process to inventory education and training (E&T) requirements and programs; identify gaps and redundancies in surface transportation owner/operator E&T; and ensure that federal training requirements support counterterrorism and infrastructure protection.
7. Implement a unified environment for sharing transportation security information that provides all relevant threat information and improves the effectiveness of information flow.
8. Reemphasize National Infrastructure Protection Plan (NIPP) framework priorities with the Sector-Specific Agencies (SSA); surface transportation owners/operators; and state, local, tribal, and territorial (SLTT) partners in order to focus development and implementation of a relevant and representative model that enhances security of the Transportation Systems Sector partners.
9. Fully identify federal roles and responsibilities in surface transportation security, taking steps to efficiently leverage resources and ultimately lead to a budget “cross cut” that extends federal coordination to include both surface transportation safety and security.
10. Identify an interagency lead to establish a single data repository for all federally obtained security risk-related information on transportation systems and assets.
11. Coordinate data requests with the established single data repository to avoid redundant efforts, take advantage of existing data sets, and establish data access control.
12. Analyze the common features of existing analysis methods and tools, and then perform a gap analysis to identify additional characteristics that would ensure that analyses are more closely comparable and consistent with the risk assessment principles in the NIPP.
13. Define a process to assess and certify extant industry risk assessments for ranking risk remediation projects under the Transit Security Grant Program or other similar federal programs.
14. Establish a fee-based, centrally managed “clearing house” to validate new privately developed security technologies that meet federal standards.

Homeland Security

15. Encourage the use of SECURE™ (Systems Efficacy through Commercialization, Utilization, Relevance, and Evaluation) and FutureTECH™ programs within appropriate directives.
16. Create a more efficient federal credentialing system by reducing credentialing redundancy, leveraging existing investments, and implementing the principle of “enroll once, use many” to reuse the information of individuals applying for multiple access privileges.
17. Collaborate with the SCCs to develop a proposal for security threat assessments standards.
18. Incorporate formal and informal methods for surface transportation owners/operators, as well as SCCs that represent them, to provide direct input into setting surface transportation research and development priorities.
19. Develop a formal, recurring surface transportation security grants process for meeting with surface transportation SCCs, owners/operators, and SLTT governments; collecting and adjudicating recommendations; and making final decisions.
20. Review key policy issues and questions identified by the Surface Transportation Security Priority Assessment to address unresolved policy issues and provide solutions for resolving identified security gaps.⁷⁰

In 2019, TSA set up a National Advisory Committee on Surface Transportation in full recognition of this means and method of transport.⁷¹ With these real threats in mind, DHS has increasingly given higher priority to commercial and industrial train and rail over the last few years, strengthened the security of the country’s freight and passenger rail systems, and reduced the risk associated with the transportation of security-sensitive materials, such as poisonous inhalation hazard (PIH) materials, certain explosive materials, and certain high-level radioactive material shipments. DHS has also formally codified the right of TSA to inspect rail facilities and equipment for these purposes. DHS works closely with a wide array of other federal agencies to carry out this purpose, including the Department of Transportation, the Federal Railroad Administration, and federal law enforcement agencies concerned about interstate crime and terrorism.⁷² DHS also depends on the cooperation of the country’s numerous freight carriers, such as CSX, Union Pacific, and others, to carry out its mission on the rails. DHS created a committee of both public and private entities to consult on rail policy. Its members include

- Association of American Railroads
- American Short Line and Regional Railroad Association
- Amtrak
- Anacostia and Pacific
- BNSF Railway Company
- Canadian National
- Canadian Pacific Railway
- CSX Transportation
- Genesee and Wyoming
- Iowa Interstate Railroad Ltd
- Kansas City Southern Railway Company
- Metra

- Norfolk Southern
- RailAmerica
- Union Pacific Railroad Company
- Wheeling and Lake Erie Railway

Both the public and the private sector are stakeholders in ensuring a safe and secure rail and mass transit system. With more than 6,000 transit service providers, commuter railroads, and long-distance trains travel daily, TSA cannot avoid this ongoing bustle. Nearly 600 transit systems operate in urban areas, while Amtrak provides passenger service on nearly 22,000 miles of track. The story for freight is even more positive.

With the lack of dependability in gasoline prices, the country's commercial and commuter lines are showing extraordinary growth in ridership. As a result of this growth, the security dynamics are intensifying. In November 2008, DHS promulgated rules that ensure a safer system, which include⁷³

- *Secure chain of custody*: Shippers will physically inspect security-sensitive materials railcars prior to shipment. The rule is applicable to 46 key urban areas.
- *Communication*: The rule requires freight and passenger railroad carriers, rail transit systems, and certain rail hazardous materials facilities to designate a rail security coordinator (RSC). The RSC will serve as the liaison to DHS for intelligence information, security-related activities, and ongoing communications with TSA.
- *Reporting security concerns*: The rule requires freight and passenger railroads to immediately report incidents, potential threats, and significant security concerns to TSA.
- *Location tracking*: The rule requires freight railroad carriers and certain rail hazardous materials shippers and receivers, at the request of TSA, to report the location of individual railcars containing security-sensitive materials within 5 minutes, and the locations of all cars containing security-sensitive materials within 30 minutes.
- *Inspection authority*: TSA is authorized to inspect freight and passenger railroad carriers, rail transit systems, and certain facilities that ship or receive specified hazardous materials by rail.

TSA, in conjunction with the Federal Transit Administration, has published specific protective measures for mass transit systems.⁷⁴ TSA will also, commencing in 2020, require all rail carriers, whether commercial or commuter, to train its staff in homeland security protocol. The program was approved in final rule form in February of 2020.⁷⁵

10.4.1 Representative Security Programs for Rail and Transit

To illustrate the emerging homeland security demands for rail, a brief look at some representative programs is in order. Whether for freight or passenger, whether operated by public or private entities, the demand for security protocols has never been greater. Indeed, DHS concluded in 2007 that rail and mass transit operations were woefully inadequate in various areas, including information sharing, research and development, public education, training and exercises, tunnels, and underwater passages (Figure 10.53).⁷⁶

Despite some predictable shortcomings, most rail and transit systems have made enormous strides in the world of homeland security. The GAO concluded that slow but sure improvements to rail security were being made but further improvements were critical to its future as an industry.⁷⁷ The GAO also concluded that the rail industry failed to share information as seamlessly as need be in matters of security and called on the industry to make improvements in this direction.⁷⁸ The array of new initiatives in rail and mass transit is beginning to make its mark in the world



Figure 10.53 An engine in the depot awaiting inspection.

of homeland security.⁷⁹ Aside from inculcating a general theory of risk assessment and mitigation, the industry sees itself as a partner with public officials. A cursory outline of these activities follows:

1. *Layers of security*: The TSA mindset on the various layers of security has now become part of the rail and mass transit approach.
2. *Transit inspectors through the Surface Transportation Security Program*: 100 officers now inspect the rail infrastructure.
3. *VIPR teams*: Using canines, advanced screening technology, and behavioral detection, the VIPR team can be dispatched to any rail location, although the program appears in the process of elimination.
4. *Grants and funding*: The rail industry as well as the public transit systems may participate in funding programs that advance security.
5. *Mobile checkpoints*: An economical way to view containers for security breaches.
6. *Site assessments*: At any location, inspectors and TSA officers can give insight and professional advice on the security and safety of an installation.
7. *Security and Emergency Preparedness Action Items*: The top 20 steps the industry must take to prepare for security risks.
8. *Training for employees*: Security awareness and skill are essential for all employees.
9. *TSA's Land Transportation Anti-terrorism Training Program (LTATP)*: Offered at FLETC.
10. *Connecting communities*: A program that highlights the unique security and emergency issues that arise in transit situations.

10.4.1.1 Amtrak

Amtrak carries out both behind-the-scenes and frontline security measures aimed at improving passenger rail security. Depending on the locale and other factors, the security practices may be uniform or random in design. Some of the common Amtrak security protocols are

- Uniformed police officers and mobile security teams
- Random passenger and carry-on baggage screening
- K-9 units
- Checked baggage screening

- On-board security checks
- Identification checks

Amtrak has also received generous funding for the safety and security of its complex infrastructure. In the Northeast corridor, Amtrak operates in diverse environments with dramatic challenges for the security operative. In 2008, DHS awarded \$25 million to Amtrak to begin the process of securing bridges, tunnels, overhangs, and other locations with target potential. That sum has either been renewed or increased until the present.⁸⁰ Preparedness grants have been regularly awarded to Amtrak and other intercity passenger rail programs since that time. In 2015, DHS provided more than \$10 million to protect critical surface transportation infrastructure and the traveling public from acts of terrorism and increase the resilience of the Amtrak rail system.⁸¹

Amtrak now deploys specialized mobile tactical units that conduct random baggage searches and other security responsibilities. The mobile security team's squads take on many forms, including armed specialized Amtrak police, explosive-detecting K-9 units, and armed counter-terrorism special agents in tactical uniforms. The mobile units were developed in conjunction with the federal, state, and private industry sectors to improve security practices. The mobile security team's procedures will not impact train schedules (Figure 10.54).

The new procedures are an enhancement to strategic security measures already in place, such as

- Uniformed police and plainclothes officers on trains and in stations
- Security cameras
- Random identification checks
- “See Something, Say Something” passenger education program to promote involvement and raise vigilance
- Investments in state-of-the-art security technology
- Security awareness training for the entire Amtrak workforce
- Behind-the-scenes activities that remain undisclosed

Amtrak is also investing in cutting-edge technologies to improve its security efforts and is presently testing intrusion detection technologies, employing explosive detection and vapor K-9 teams, conducting more passenger screenings, and actively participating in the joint terrorism task forces in its various regions.⁸² Finally, Amtrak is calling on its customer base to be active



Figure 10.54 Amtrak's Mobile Tactical Unit helps secure the railways.

Homeland Security

players in the security effort. Through its Partners for Amtrak Safety and Security (PASS) program, customers are asked to be active participants in the who, what, where, when, and how of criminal conduct.

Internet Exercise: Learn about the PASS program at <https://pass.amtrak.com>.

10.4.1.2 CSX: The Freight Line

Just as the public rail entities have core responsibilities, so too do the private rail companies. CSX is an excellent example of a progressive freight shipper with a massive route network in the eastern half of the United States. It, like all other rail concerns, has had to reconsider how it carries out its business since 9/11. As noted, shipments of hazardous and security-sensitive materials are subject to a host of regulations and other requirements.⁸³ Railroads also must

- Compile security data based on commodity and route type
- Identify security vulnerabilities
- Identify alternative routes
- Develop programs of safety and security
- Revisit route selections
- Communicate with state and federal officials
- Design tracking systems for sensitive material
- Work in unity with the motor carriers whose cargo the rail transports

See Figure 10.55⁸⁴ for a map of CSX's rail system.

CSX, just as its sister carriers, abides by a host of regulations. Of recent interest are the TSA requirements that shipments to designated urban areas be processed according to new protocols, and additionally, that the chain of custody of these shipments be tracked. The materials subject to the rules include explosives, toxic inhalation hazard (TIH) materials, PIH materials, and bulk amounts of radioactive materials, all of which are now designated rail security-sensitive materials.

TSA now insists that certain rail secure areas be the exclusive points of shipping or receiving. As of February 15, 2009, rail companies, such as CSX, are only able to accept shipments of rail security-sensitive materials from rail secure areas. In areas designated high-threat urban areas (HTUA), delivery will only be possible to a rail secure area.

Another facet of the new rules on rail shipments will involve written certifications of compliance. Shipments of rail security-sensitive materials are subject to TSA chain-of-custody requirements. The rules require (1) all consignors and (2) those consignees located in an HTUA to have personnel physically present for attended handoffs of all railcars containing rail security-sensitive materials. TSA has promulgated that it expects the personnel attending the handoff of railcars with rail security-sensitive materials to document the transfer by recording (1) each railcar's initials and number, (2) the individuals attending the transfer, (3) the location of the transfer, and (4) the date and time of the transfer. Contending with new rules of the road will be an ongoing demand for the freight industry (Figure 10.56).

Internally, CSX has established a sophisticated and impressive security and safety program. Aside from its materials training, emphasis on employee safety, and other industrial applications, CSX fully comprehends the mix of the public and private interests in its rail operation. The line shares information with governmental entities and partners, with myriad agencies dedicated to safety and security. Examples of these efforts are

- *CSX Transportation's (CSXT) Network Operations Workstation (NOW):* A cornerstone of this partnership is CSXT's sharing of its highly specialized secure NOW system. Key highlights of the NOW system include

10.4 Rail and Mass Transit

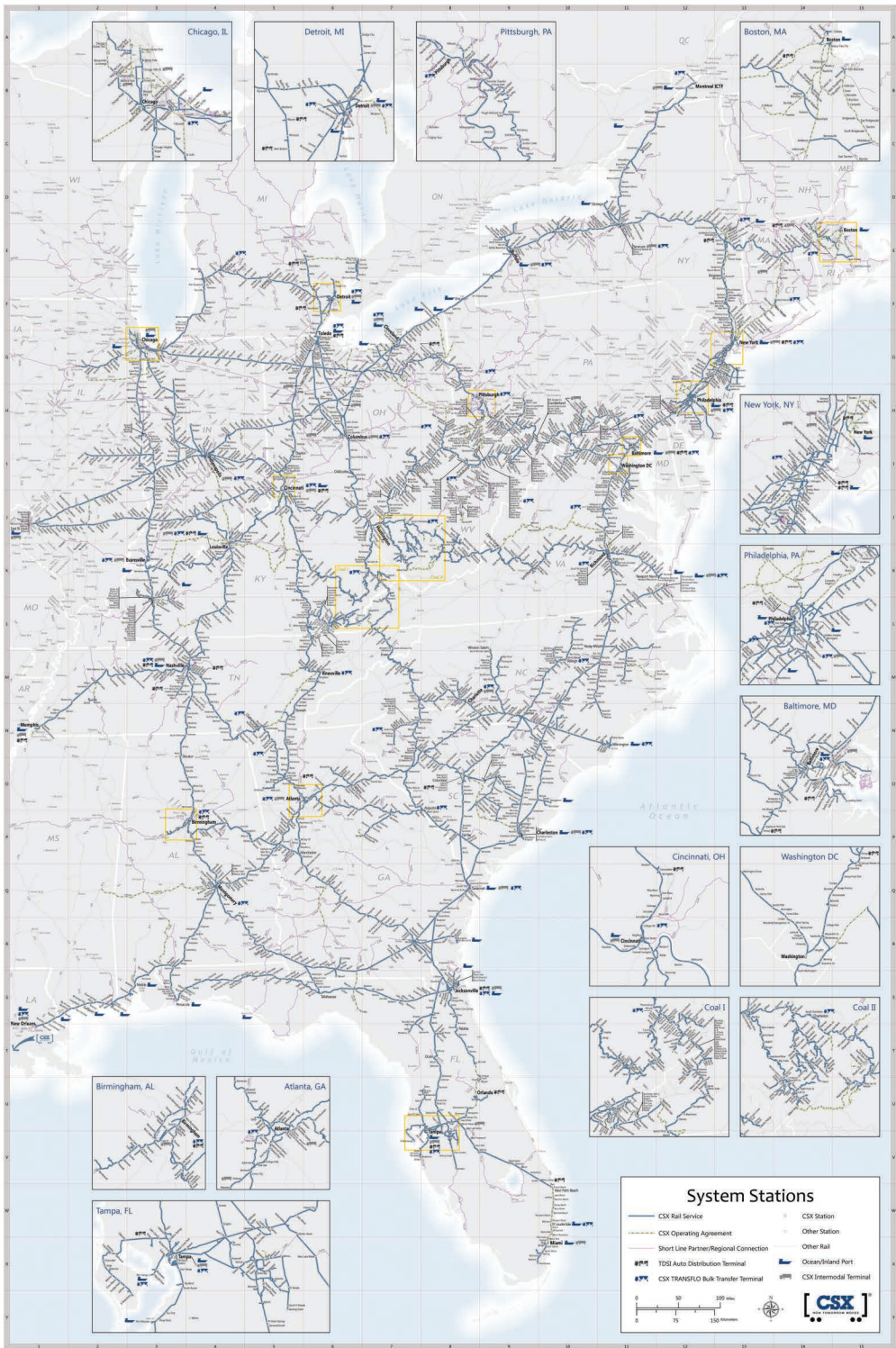


Figure 10.55 CSX rail system map.



Figure 10.56 CSX freight train.

- *Enhanced monitoring*: Provides state homeland security and law enforcement officials with a tool to identify the status of CSXT trains and railcars in each state. Before, officials needed to call CSXT to access this information.
- *Information sharing*: Helps security officials prepare for and, if needed, respond to emergency situations.
- *Targeted security*: With additional information about what is carried on rails, state officials can more efficiently allocate law enforcement resources, coordinate with CSXT security officials, and integrate rail security into ongoing law enforcement operations.
- *Joint law enforcement and emergency responder training*: Law enforcement officials train with the CSXT Police Rapid Response Team—a group of highly skilled police officers specifically trained to respond to security incidents. Additionally, state and community emergency first responders train alongside CSXT's experts in hazardous materials and emergency response.
- *Sharing of hazardous materials density studies*: These data help emergency response organizations plan their resources and identify the types of emergency response training applicable to their jurisdiction.
- *Closer coordination of law enforcement operations in and around CSXT yards*: CSXT can provide its partners with around-the-clock access to its rail security professionals.
- *Developing better rail security policies*: States and CSXT continue to work with policymakers to identify important public policy issues that can impact and improve rail security.

CSX, like its counterparts in the industry, sees the world in differing terms than pre-9/11. The industry works closely with local, state, and federal authorities to secure the nation's railroads. Freight railroads remain in constant communication with the U.S. Department of Transportation security personnel, the FBI, the National Security Council, and state and local law enforcement officers.

10.4.1.3 SEPTA: Rail Mass Transit

The Southeastern Pennsylvania Transit Authority (SEPTA) is one of the nation's largest rail commuter systems. It also connects and collaborates with other carriers and is part and parcel



Figure 10.57 SEPTA's Wilmington, Delaware station.

of a very large collective of mass transit providers, including New Jersey Transit, Delaware Area Transit, and Amtrak. The system can readily and very easily hook up the rider to New York, Baltimore, and Washington, DC. In this extreme congestion, SEPTA needs to always be mindful of the security threat (Figure 10.57).

Prevention of future terrorist attacks is both a national and a local concern. SEPTA takes the threat of terrorism very seriously. Passengers are afforded maximum security and protection. Increased presence of transit police officers on the system's cars and stations has been a high priority for SEPTA management. Also present throughout the transit system, although obviously less visible, is a trained team of undercover, plainclothes SEPTA police officers who are working to ensure the security of our passengers.

SEPTA's police officers have been thoroughly trained in antiterrorism awareness. Specially trained officers have instructed additional SEPTA personnel in an antiterrorism program that includes recognition, response, and prevention techniques.

Internet Exercise: Learn about careers in law enforcement in SEPTA at <http://autohire.careershop.com/septajobs/default.asp?ContentID=7>.

See Figure 10.58 for a route map from SEPTA.

Yet when one considers the sheer volume of passengers on this system day to day, are these general recommendations enough? Does a transit police force have the capability to trace and track every imaginable threat? Is the geography alone too much to cover? Most observers of mass transit indicate there are simply too many holes in the dike to be confident about thwarting the terrorist threat—and just as frustratingly, too many players in the overall mix. To be successful, mass transit systems will have to be better organized. Here are some suggestions:

TSA's 17 Security and Emergency Preparedness Action Items

1. Establish written System Security Programs and Emergency Management Plans.
2. Define roles and responsibilities for security and emergency management.
3. Ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control.
4. Coordinate Security and Emergency Management Plan(s) with local and regional agencies.
5. Establish and maintain a security and emergency training program.

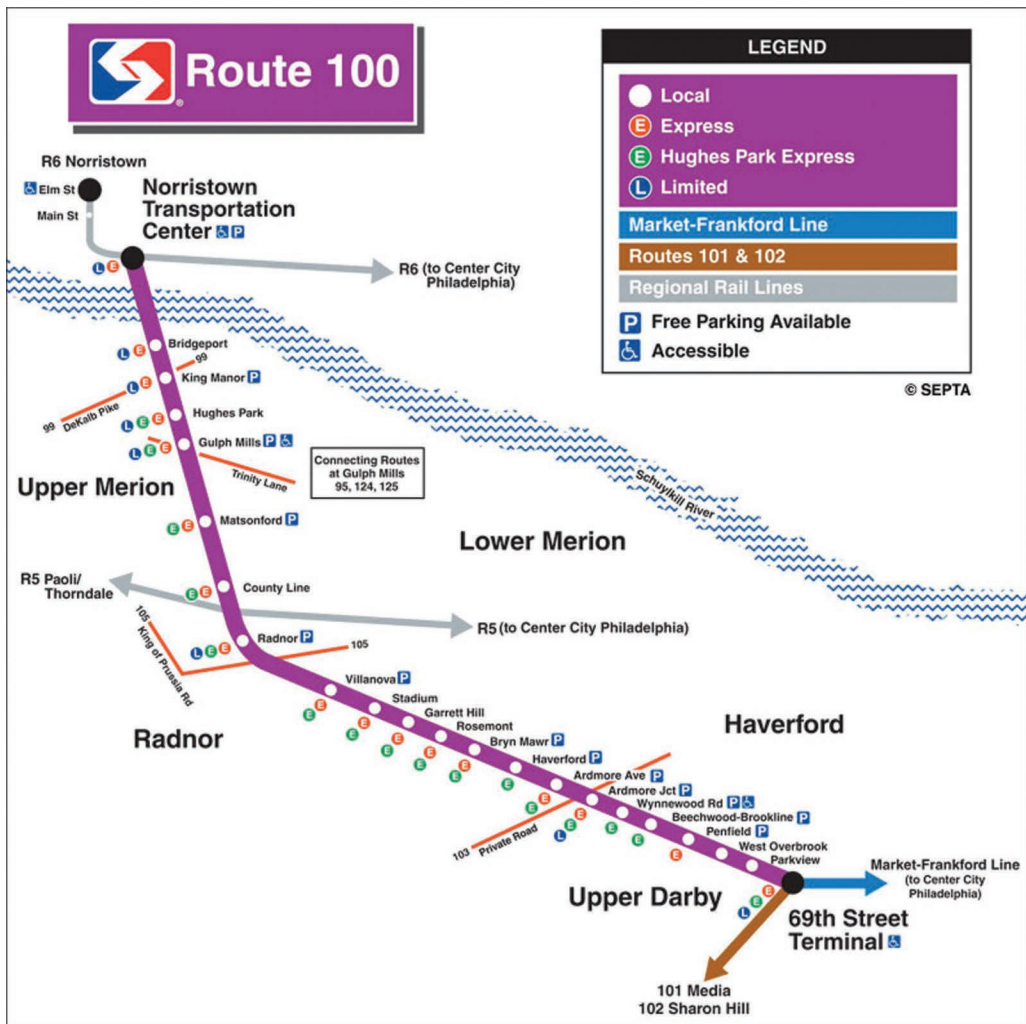


Figure 10.58 Railway route map. (From Southeastern Pennsylvania Transport Authority. Maps and stations. <http://www.septa.org/maps/>.)

6. Establish plans and protocols to respond to the DHS Homeland Security Advisory System threat levels.
7. Implement and reinforce a public security and emergency awareness program.
8. Conduct tabletop and functional drills.
9. Establish and use a risk management process to assess and manage threats, vulnerabilities, and consequences.
10. Participate in an information-sharing process for threat and intelligence information.
11. Establish and use a reporting process for suspicious activity (internal and external).
12. Control access to security-critical facilities with identification badges for all visitors, employees, and contractors.

13. Conduct physical security inspections.
14. Conduct background investigations of employees and contractors.
15. Control access to documents of security-critical systems and facilities.
16. Implement a process for handling and access to sensitive security information.
17. Conduct security program audits.⁸⁵

While all of the recommendations are poignant, the training side of the security and risk plan cannot be forgotten or neglected. In every facet of mass transit, the risk to passengers and employees is high. Those entrusted with transit operation must be sure to train the employees to the highest level. TSA has devised an excellent matrix of learning to assure that the essential subject matter is covered and that costs are contained (Figure 10.59).

10.5 Conclusion

Transportation runs heavily throughout the pages of this chapter. More specifically, the chapter delves into the full menu of TSA activities. The most visible of homeland departments, TSA, is now part of the fabric of travel and travel installations. Usually associated with airports, TSA has additional responsibilities involving public roads, bridges, rail, pipelines, and train stations. At its base, TSA is responsible for transportation threat assessment and vulnerability, the promulgation of standards and practices regarding safety and security, and the anticipation of novel innovations in the homeland dimension. Trace portals, millimeter-wave machines, and biometrics are examples of how technology impacts TSA operations. TSA adopts a policy of layered security, whereby at various stages of security scrutiny it is unlikely that a terrorist will escape each and every level of oversight.

Other transportation initiatives highlighted in this chapter include the federal air marshal, federal flight deck officers, and law enforcement officers flying armed. Each of these programs provides an added layer of armed protection in the air travel industry. TSA employs canines in various components of its practices, especially regarding explosives.

The chapter looks intently on how homeland functions are pertinent to the maritime world. The prevention of terrorist attacks on maritime critical infrastructure, the safeguarding of oceans and corresponding resources, and the minimization of economic losses in the maritime domain are highly relevant homeland functions. In implementing the National Strategy for Maritime Security, DHS operatives accept the broad-based perspective on what constitutes the maritime domain and rely heavily on the maritime industry to advise as to best practices. In maritime security, government and commerce work collaboratively. Featured with rightful relevancy is the role and function of the U.S. Coast Guard, which naturally operates in the maritime. The Coast Guard, as part of its core mission, provides maritime safety and security in multiple contexts. In addition, the Coast Guard needs to maintain mobility in waterways and other ports of interest, assist in the protection of natural resources, respond to emergencies and catastrophes, and is part of the U.S. national defense. In each of these categories, the Coast Guard's history displays extraordinary success. Saving thousands of lives is simply the mission, a Coastie would argue. Aside from the endless plucking of victims from water peril, the Coast Guard operates the premier SAR team—legendary in both requirements and results. The Coast Guard wears comfortably the hat of law enforcement as well, by targeting smugglers and drug traffickers, terrorists, and other undesirables. The Coast Guard operates a specialized facility to train its members in law enforcement functions—the Maritime Law Enforcement Academy in Charleston, South Carolina. The sweep of Coast Guard services is difficult to fully catalog since, aside from all these functions, the command deals with port and harbor protections, container

Training description	Focus	Categories of employees to receive								Total training cost	
		Front line employees	Station managers	Administrative and support staff	Maintenance workers	Mid-Level management	Senior management	Operations control center staff	Security guards		Law enforcement
Security awareness	Enhance capability to identify, report, and react to suspicious activity and security incidents										\$0
Behavior recognition	Recognize behaviors associated with terrorists' reconnaissance and planning activities, including the conduct of surveillance. Applies lessons learned from the Israeli security meeting.										\$0
Immediate emergency response	Prepare passenger rail train operators to deal with explosive detonations, incendiaries, released chemical hazards, and similar threats in the confines of trains and system infrastructure.										\$0
National incident management system (NIMS)	Ensure transit agency emergency preparedness and response personnel gain and retain the knowledge and skills necessary to operate under NIMS in accordance with the National Response Plan (NRP).										\$0

Figure 10.59 Basic mass transit security training program. (From Transportation Security Administration, www.tsa.gov.)

(Continued)

Training description	Focus	Categories of employees to receive								Total training cost	
		Front line employees	Station managers	Administrative and support staff	Maintenance workers	Mid-Level management	Senior management	Operations control center staff	Security guards		Law enforcement
Operations control Center readiness	Identify security vulnerabilities. Understand and exercise role of OCC personnel in preventing terrorist attacks. Distinguish characteristics of improvised explosive devices (IEDs) and weapons of mass destruction. Specify priorities during a terrorist attack and manage incident response. Apply transit agency's operational plans for response to IED and WMD scenarios, directing and coordinating activities in the system.									\$0	
		Mass transit security follow-on courses									
Training description	Focus	Front line employees	Station managers	Administrative and support staff	Maintenance workers	Mid-Level management	Senior management	Operations control center staff	Security guards	Law enforcement	Total training cost
Management of transit emergencies I (4-day course)	Ensure employees throughout the transit agency understand individual roles in emergency response and the transit system's role in emergencies or disasters in the system and the broader community.										\$0

Figure 10.59 (CONTINUED) Basic mass transit security training program. (From Transportation Security Administration, www.tsa.gov.)

(Continued)

Management of transit emergencies II (1-day course)	Ensure employees throughout the transit agency understand individual roles in emergency response and the transit system's role in emergencies or disasters in the system and the broader community.									\$0
Coordinated interagency emergency response	Advance interoperability of the transit agency with multiple responding entities in emergency response.									\$0
Managing counterterrorism programs	Enable transit agency management officials to develop and manage a counterterrorism program in a transit system.									\$0
Prevention and mitigation— IEDS and WMD: T4 3-day course	Enhance capabilities to identify threats from improvised explosive devices and weapons of mass destruction (chemical, biological, radiological, nuclear) to identify, report, and react to suspicious activity and security incidents									\$0

Figure 10.59 (CONTINUED) Basic mass transit security training program. (From Transportation Security Administration, www.tsa.gov.)

(Continued)

Training description		Focus	Mass transit security follow-on courses								Total training cost	
			Front line employees	Station managers	Administrative and support staff	Maintenance workers	Mid-Level management	Senior management	Operations control center staff	Security guards	Law enforcement	
Prevention and Mitigation— IEDS and WMD: CBRNE Incident Management 1-day course		Enhance capabilities to identify threats from improvised explosive devices and weapons of mass destruction (chemical, biological, radiological, nuclear) to identify, report, and react to suspicious activity and security incidents.										\$0
Transit vehicle hijacking prevention and response		Enable employees to develop and implement plans and procedures to respond to transit vehicle hijackings and workplace violence.										\$0
Integrated anti-terrorism security program		Enhance capabilities of transit agency security officials, law enforcement personnel, and others with interaction with passengers to detect, deter, and prevent acts of terrorism.										\$0
Transit system security design		Expand integration of security considerations into designs of new transit systems and improvements of existing systems.										\$0

Figure 10.59 (CONTINUED) Basic mass transit security training program. (From Transportation Security Administration, www.tsa.gov.)

(Continued)

Train-the-trainer courses										
Training description	Focus	Categories of employees to receive							Total training cost	
		Front line employees	Station managers	Administrative and support taff	Maintenance workers	Mid-Level management	Senior management	Operations control center staff		Security guards
Security a wareness train-the-trainer	Enhance capability to identify, report, and react to suspicious activity and security incidents.									\$0
Behavior recognition train-the-trainer	Recognize behaviors associated with terrorists' reconnaissance and planning activities, including the conduct of surveillance. Applies lessons learned from the Israeli security meeting.									\$0
Total training costs—all courses										

Figure 10.59 (CONTINUED) Basic mass transit security training program. (From Transportation Security Administration, www.tsa.gov.)

and vessel inspection, offshore drilling facilities, cargo safety, and environmental crimes. The Coast Guard's Homeport program encompasses all of these activities.

Finally, the chapter takes a close look at the rail and mass transit industry. While rail is both publicly and privately operated, the types of mass transit make full coverage an impossibility. Hence, the stress here is on rail, due to its potential to be a medium of delivery for the terrorist, or the locus with the most potential for human loss of life. As in Spain a few years ago, the compelling and hideous impact of a terrorist on a train system has unfortunately been displayed. How Amtrak, CSX, and the SEPTA system address the many challenges of homeland security is fully assessed.

Keywords

Baggage Screening; Boarding Officer; Canine Explosive Detection Unit; Cargo and Facilities Division; Certificate of Operation; Container Inspection Training and Assistance Team; Department of Commerce; Federal Air Marshal; Federal Aviation Administration; Federal Flight Deck Officer; Federal Highway Administration; Inspection and Compliance Directorate; Law Enforcement Officer Flying Armed; Maritime Security; Mass Transit; Millimeter Wave; Mobile Tactical Unit; National Strategy for Maritime Security; National Vessel Documentation Center; Operation Homeport; Operation Noble Eagle; Passenger Screening; Poisonous Inhalation Hazard; Rail Secure Area; Rail Security-Sensitive Material; Rail Transit System; Registered Traveler Program; Search and Rescue Team; Security Threat Assessment; Toxic Inhalation Hazard; Trace Portal; Transportation Security; Transportation Security Administration

Discussion Questions

1. The Coast Guard Container Inspection Program assumes much about our trading partners. Comment.
2. In what way has trade and commerce benefited from electronic tracking and computer systems?
3. Some argue that U.S. Citizenship and Immigration Services is delving into activities best left to other historic agencies. Can you identify an example of where this criticism might be relevant?
4. TSA is often labeled a reactive agency that gives little thought to its practices. Do you think this conclusion is reasonable in any sense?
5. Why does TSA have such turnover problems in personnel?
6. Explain why the layered security practice of TSA works so effectively.
7. How should TSA be a leader in the use of technology and computer innovation in its practices?
8. How do biometric measures replace human function and task?
9. The Coast Guard is often labeled as an entity being asked to do everything and even more. How is this so? And how has this condition led to stresses in the Coast Guard?
10. Discuss some of the more recent plans and programs designed for the maritime world.

Homeland Security

11. Discuss three programs of the Coast Guard that deal with vessels and law enforcement function.
12. Why is rail and mass transit rail such a difficult industry in which to apply uniform standards?
13. Of the three types of rail systems—namely, freight, passenger, and public mass transit—which has the greatest demands when it comes to security issues?

Practical Exercises

1. Evaluate TSA's 20 layers of security. Which could readily be eliminated and why?
2. Prepare a career file with representative positions for the following occupations:
 - Federal air marshal
 - Federal flight deck officer
 - TSA
 - TSA canine
3. Review the career options in the Coast Guard. Explain how many of the career paths deal with homeland security. Provide at least three examples.
4. Prepare a mock vessel inspection request for the U.S. Coast Guard.
5. Contact your local mass transit provider. Find out what steps the entity has taken relative to homeland security preparedness.

Notes

- 1 K. Vlahos, Pat-down dust-up renews screening debate, *Homeland Security Today* (June, 2011): 10–11.
- 2 TSA, Social media, https://www.tsa.gov/news/social_media (accessed August 22, 2020).
- 3 For some representative examples of TSA abuse and unprofessionalism, visit the following links: Failure rate of inspections at airport facilities: K. Pavlich, Surprise: TSA hasn't improved since failing 95 percent of security tests, *Townhall*, November 4, 2015, <http://townhall.com/tipsheet/katiepavlich/2015/11/04/surprise-tsa-is-still-sucking-terribly-n2075370> (accessed August 22, 2020); J. Fishel, P. Thomas, M. Levine, and J. Date, Undercover DHS tests find security failures at US airports, *ABC News*, June 1, 2015, <http://abcnews.go.com/US/exclusive-undercover-dhs-tests-find-widespread-security-failures/story?id=31434881> (accessed August 22, 2020); on the failure rate on weapons and explosives: E. Bradner and R. Marsh, Acting TSA director reassigned after screeners failed tests to detect explosives, weapons, *CNN*, June 2, 2015, <http://www.cnn.com/2015/06/01/politics/tsa-failed-undercover-airport-screening-tests> (accessed August 22, 2020); on TSA as an institutional failure as an operating agency: M. Fox, TSA a failure at every level: Security expert, *CNBC*, June 9, 2015, <http://www.cnbc.com/2015/06/09/tsa-a-failure-at-every-level-security-expert.html> (accessed August 22, 2020).
- 4 For a complete listing of cases among TSA employees, see <https://www.tsa.gov/coronavirus> (accessed August 22, 2020).
- 5 E. Ashford, More than a revenue source, *Community College Daily*, September 11, 2015, <https://www.maricopacorporate.com/corporate-training/news/more-revenue-source> (accessed August 22, 2020).
- 6 TSA Organizational Chart, https://www.tsa.gov/sites/default/files/tsa_org_chart_matrix.pdf (accessed August 22, 2020).

- 7 Transportation Security Administration, Mission, <https://www.tsa.gov/about/tsa-mission> (accessed August 22, 2020).
- 8 There have been increasing, unrelenting calls for the TSA to be privatized; see: C. Edwards, Privatizing the transportation security administration, *Policy Analysis*, 742 (November 19, 2013), http://object.cato.org/sites/cato.org/files/pubs/pdf/pa742_web_1.pdf (accessed August 22, 2020); Privatizing is a means and method for cost savings since the TSA salaries and demands are significantly higher. See: E. Katz, Trump Administration Freezes Transportation Security Administration Hiring, Government Executive, February 26, 2020, <https://www.govexec.com/management/2020/02/trump-administration-freezes-tsa-hiring/163350/> (accessed August 22, 2020).
- 9 See: Pittsburgh International Airport, PIT Safe Travels Program, <https://flypittsburgh.com/pittsburghinternational-airport/terminal-information/safety-security/covid19/pitsafetravels/> (accessed August 22, 2020).
- 10 See: TSA, TSA by the Numbers Fact Sheet, https://www.tsa.gov/sites/default/files/resources/tsabythenumbers_factsheet.pdf (accessed August 22, 2020).
- 11 C. J. Ciaramella, Abolish the TSA, *The Washington Post*, April 16, 2015, https://www.washingtonpost.com/posteverything/wp/2015/04/16/abolish-the-tsa/?utm_term=.bcb5d054cad8 (accessed August 22, 2020).
- 12 See: J. Price, Getting rid of VIPR, TSA exit lane personnel, and \$46 million in airport security improvement money-is this a good idea? The Airport Writer, February 20, 2020, <https://leadingedgestrategies.com/getting-rid-of-vipr-tsa-exit-lane-personnel-and-46-million-in-airport-security-improvement-money-is-this-a-good-idea/> (accessed August 22, 2020).
- 13 See also: Dept. of Homeland Security, If you See Something, Say Something Campaign Partnership Guide, https://www.dhs.gov/sites/default/files/publications/SeeSay-Overview508_1.pdf (accessed August 22, 2020).
- 14 TSA, Screening Partnership Program Factsheet, https://www.tsa.gov/sites/default/files/resources/spp_factsheet.pdf (accessed August 22, 2020).
- 15 See: TSA Website, For Industry-Training webpage, <https://www.tsa.gov/for-industry/training> (accessed August 22, 2020).
- 16 See: TSA Website, Travel-Law Enforcement webpage, <https://www.tsa.gov/travel/law-enforcement> (accessed August 22, 2020).
- 17 Statement of Jennifer Grover, acting director, Homeland Security and Justice, Explosives detection canines: TSA has taken steps to analyze canine team data and assess the effectiveness of passenger screening canines (Testimony before the Subcommittee on Transportation Security, Committee on Homeland Security, House of Representatives), GAO-14-695T, June 24, 2014, <http://www.gao.gov/assets/670/664331.pdf> (accessed August 22, 2020).
- 18 See also: US Dept of Homeland Security, REDDI – the Regional Explosives Detection Dog Initiative, https://www.dhs.gov/sites/default/files/publications/st_19_0627_reddi_factsheet-508.pdf (accessed August 22, 2020).
- 19 US Dept. of Homeland Security, Snapshot: S&T and the Pentagon are Changing K-9 Bomb Detection, <https://www.dhs.gov/science-and-technology/news/2017/09/12/snapshot-st-and-pentagon-are-changing-k-9-bomb-detection> (accessed August 22, 2020).
- 20 See: TSA, TSA Canine Training Center Factsheet, https://www.tsa.gov/sites/default/files/resources/caninetrainingcenter_factsheet_0.pdf (accessed August 22, 2020).
- 21 GAO, Aviation security: TSA has made progress, but additional efforts are needed to improve security, *GAO Highlights*, 2011.
- 22 A. Sternstein, Experts chide TSA for poor risk assessment of security measures, NextGov.com, September 30, 2011, <http://www.nextgov.com/technology-news/2011/09/experts-chide-tsa-for-poor-risk-assessment-of-security-measures/49866> (accessed August 22, 2020); See also: GAO, Aviation security: A national strategy and other actions would strengthen TSA's efforts to secure commercial airport perimeters and access controls, September 30, 2009, <http://www.gao.gov/assets/300/296396.pdf> (accessed August 22, 2020).
- 23 See: D. Thornton, How TSA jump-started enterprise risk management, *Federal News Network*, July 29, 2016, <https://federalnewsnetwork.com/management/2016/07/tsa-jump-started-enterprise-risk-management/> (accessed August 22, 2020).

Homeland Security

- 24 TSA, *Enterprise Risk Management: ERM Policy Manual* (August 2014), 8, <https://www.aferm.org/wp-content/uploads/2015/10/TSA-ERM-Policy-Manual-August-2014.pdf> (accessed August 22, 2020).
- 25 TSA, Innovation Task Force webpage, <https://www.tsa.gov/itf> (accessed August 22, 2020).
- 26 For a new program under production, see the Apex Screening at Speed program at: https://www.dhs.gov/sites/default/files/publications/Apex%20Screening%20at%20Speed%20508%20Approved%20Final_0.pdf (accessed August 22, 2020).
- 27 The TSA Blog, TSA travel tips Tuesday: Traveling with personal medical electronic devices, February 25, 2014, <http://blog.tsa.gov/2014/02/tsa-travel-tips-tuesday-blog-post.html> (accessed August 22, 2020).
- 28 Privacy problems sprinkle throughout the world of DHS and homeland defense. See B. K. Collins and H. Morrow, Using shared technology in bioterrorism planning and response: Do privacy laws affect administrative judgments? *The Homeland Security Review*, 4 (2010): 43.
- 29 DHS, Privacy assessment update for TSA advance imaging technology, December 18, 2015, <https://www.dhs.gov/sites/default/files/publications/privacy-tsa-pia-32-d-ait.pdf> (accessed August 22, 2020).
- 30 DHS, Privacy impact assessment update for TSA advanced imaging technology, January 25, 2011, <http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf> (accessed August 22, 2020).
- 31 Article—The Sky's the Limit, Article—Asking the Right Questions; DHS, Privacy impact assessment update for TSA advanced imaging technology, January 25, 2011, <http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf> (accessed August 22, 2020).
- 32 See: TSA, TSA by the Numbers Fact Sheet, https://www.tsa.gov/sites/default/files/resources/tsabythenumbers_factsheet.pdf (accessed August 22, 2020).
- 33 TSA, Press Release: TSA launches 3D checkpoint scanning technology demonstration at two airports, June 15, 2107, <https://www.tsa.gov/news/press/releases/2017/06/15/tsa-launches-3d-checkpoint-scanning-technology-demonstration-two> (accessed August 22, 2020).
- 34 Biometrics.gov, Introduction to biometrics, 1, <http://www.biometrics.gov/Documents/BioOverview.pdf> (accessed August 22, 2020).
- 35 P. Wolfhope, Mobile biometric devices: What the future holds, *The Police Chief* (September, 2011): 38–40.
- 36 See: Dept of Homeland Security, Highlight-Facial Recognition Technology, April 2019, https://www.dhs.gov/sites/default/files/publications/FacialRecognition-HLT_0409-508.pdf (accessed August 22, 2020).
- 37 See also: *Ibid.*
- 38 FBI, About the Biometric Center of Excellence, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/about/about-the-biometric-center-of-excellence (accessed August 22, 2020).
- 39 Dept of Homeland Security, Trusted Traveler Programs, <https://ttp.dhs.gov/> (accessed August 22, 2020).
- 40 US Customs and Border Protection, Trusted Traveler Programs – Schedule Appointment for Global Entry, <https://ttp.dhs.gov/schedulerui/schedule-interview/location?lang=en&vo=true&returnUrl=ttp-external&service=UP> (accessed August 22, 2020).
- 41 DHS, Privacy impact assessment update for the credential authentication technology/boarding pass scanning system, August 11, 2009, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_catbpss.pdf (accessed August 22, 2020).
- 42 J. Wade, Maritime security, *Risk Management*, 52 (December 2005): 40.
- 43 A. G. Grynkewich, Maritime homeland defense, *Air and Space Power Journal* (Winter 2007): 86.
- 44 Maritime Transportation Security Act of 2002, P.L. 107–295, *U.S. Statutes at Large* 116, 2002: 2064.
- 45 Office of the President, *The National Strategy for Maritime Security* (Washington, DC: U.S. Government Printing Office, 2005), <https://georgewbush-whitehouse.archives.gov/homeland/maritime-security.html> (accessed August 22, 2020).
- 46 At present there is a good bit of discussion as to the future structure and organization of maritime domain awareness. Dept. of Homeland Security, National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security, https://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf (2005) (accessed August 22, 2020).

- 47 US Coast Guard, Missions webpage, <https://www.work.uscg.mil/Missions> (accessed August 22, 2020).
- 48 U.S. Coast Guard, SAR program information, <https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Response-Policy-CG-5R/Office-of-Incident-Management-Preparedness-CG-5RI/US-Coast-Guard-Office-of-Search-and-Rescue-CG-SAR/CG-SAR-1/SAR-Program-Information/> (accessed August 22, 2020).
- 49 U S Coast Guard, Annual Performance Report, 14 (2017), <https://www.uscg.mil/Portals/0/documents/budget/FY17%20APR%2015%20May%2018%20-%20Final%20-%20POSTED.pdf> (accessed August 22, 2020).
- 50 14 U.S. Code, section 2, 2008.
- 51 President's Council on Integrity and Efficiency, *Quality Standards for Investigations* (Washington, DC: U.S. Government Printing Office, 2003), 17, <https://www.ignet.gov/sites/default/files/files/invprg1211appi.pdf> (accessed August 22, 2020).
- 52 U.S. Coast Guard, Office of Counterterrorism and Defense operations policy: Ports, waterways and coastal security, <https://www.gocoastguard.com/about-the-coast-guard/discover-our-roles-missions/ports-waterway-security> (accessed August 22, 2020).
- 53 Dept of Homeland Security, Air Cargo Screening Program, <https://www.dhs.gov/sites/default/files/publications/Air%20Cargo%20Fact%20Sheet%20508%20Approved%20Final%2011OCT16.pdf> (accessed August 22, 2020).
- 54 D. Philpott, Improving the security of U.S. harbors and seaports, *Homeland Defense Journal* (November 2007): 31
- 55 K. L. Walters III, Industry on alert: Legal and economic ramifications of homeland security act on maritime commerce, *Tulane Maritime Law Journal*, 30 (2006): 311.
- 56 Walters, Industry on alert, 334–335.
- 57 M. Florestal, Terror on the high seas: The trade and development implications of the U.S. National Security Measures, *Brooklyn Law Review*, 72 (2007): 441.
- 58 See: US Coast Guard, CG-FAC: Office of Part & Facility Compliance, <https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/fac2/> (accessed August 22, 2020).
- 59 GAO, *Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies* (Washington, DC: U.S. Government Printing Office, 2008), 1, <http://www.gao.gov/new.items/d0812.pdf> (accessed August 22, 2020).
- 60 US Coast Guard, Facility, Vulnerability and Security Measures Summary form, CD-6025, <https://www.reginfo.gov/public/do/DownloadDocument?objectID=7516101> (accessed August 22, 2020).
- 61 GAO, *Homeland Security: Challenges Facing the Coast Guard as It Transitions to a New Department* (Washington, DC: U.S. Government Printing Office, 2003), 1, <http://www.gao.gov/new.items/d03467t.pdf> (accessed August 22, 2020).
- 62 American Public Transportation Association, 2019 Public Transportation Fact Book, 9 (2019), https://www.apta.com/wp-content/uploads/APTA_Fact-Book-2019_FINAL.pdf (accessed August 22, 2020).
- 63 Amtrak, FY 2019 Company Profile, https://media.amtrak.com/wp-content/uploads/2020/06/Amtrak-Corporate-Profile_FY2019_-FINAL-033120.pdf (accessed August 22, 2020).
- 64 R. C. Paolino, All aboard: Making the case for a comprehensive rerouting policy to reduce the vulnerability of hazardous rail-cargoes to terrorist attack, *Military Law Review*, 193 (2007): 144.
- 65 From: American Public Transportation Association (APTA), 2013 *Public Transportation Fact Book* (Washington, DC: APTA, 2013), 11, <https://www.apta.com/wp-content/uploads/Resources/resources/statistics/Documents/FactBook/2013-APTA-Fact-Book.pdf> (accessed August 22, 2020).
- 66 J. Plant, Terrorism and the railroads: Redefining security in the wake of 9/11, *Review of Policy Research*, 293 (2004): 301.
- 67 J. Plant, Terrorism and the railroads, 301.
- 68 Waiting for al-Qaeda's next bomb, *The Economist* (May 3, 2007): 29; A. Loukaitou-Sideris et al., Rail transit security in an international context: Lessons from four cities, *Urban Affairs Review*, 41(6) (2006): 21; B. Johnstone, *New Strategies to Protect America: Terrorism and Mass Transit after London and Madrid* (Washington, DC: Center For American Progress, 2005), 21; M. Sanadjian, Fear, terror, and the new global economy of salvation-global excess and “suicide” bombing of London, *Social Identities*, 12(6) (2006): 701–725.

Homeland Security

- 69 APTA, 2019 FactBook, at 2–3.
- 70 The White House, *Surface Transportation Security Priority Assessment*, March 2010, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/STSA.pdf (accessed August 22, 2020).
- 71 See: TSA National Press Release, TSA announces the establishment of the Surface Transportation Security Advisory Committee, April 8, 2019, <https://www.tsa.gov/news/press/releases/2019/04/08/tsa-announces-establishment-surface-transportation-security-advisory> (accessed August 22, 2020).
- 72 Congressional Research Service, *Transportation Security: Issues for the 112th Congress*, February 1, 2011, <http://www.fas.org/sgp/crs/homesec/RL33512.pdf> (accessed August 22, 2020).
- 73 Net railroad income correlates to railroad spending on capital and maintenance expenditures. Capital spending plus maintenance costs. Data are for Class I railroads. p = Preliminary Association of American Railroads (AAR), <https://www.aar.org/rail-cost-indexes/> (accessed August 22, 2020).
- 74 Review this comprehensive list of recommendations in the document from November 2006 entitled Transit Agency Security and Emergency Management Protective Measures, <http://www.trb.org/Main/Blurbs/158319.aspx> (accessed August 22, 2020).
- 75 See: Security Training for Surface Transportation Employees, 85 FR 16456 (2020), <https://www.federalregister.gov/documents/2020/03/23/2020-05126/security-training-for-surface-transportation-employees> (accessed August 22, 2020).
- 76 DHS, Transportation systems: Critical infrastructure and key resources sector specific plan as input to the National Infrastructure Protection Plan A81-81, 2007, <https://www.hsd1.org/?view&did=474328> (accessed August 22, 2020).
- 77 GAO, Rail security: TSA improved risk assessment but could further improve training and information sharing, June 14, 2011, <http://www.gao.gov/assets/130/126419.html> (accessed August 22, 2020).
- 78 GAO, *Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach* (Washington, DC: GAO, September 2010), <http://www.gao.gov/new.items/d10895.pdf> (accessed August 22, 2020); see also: *Transportation Security Administration: Surface Transportation Inspector Activities Should Align More Closely with Identified Risks* (Washington, DC: GAO, December 2017), <https://www.gao.gov/products/GAO-18-180> (accessed August 22, 2020).
- 79 GAO, *Positive Train Control: Additional Oversight Needed as Most Railroads Do Not Expect to Meet 2015 Implementation Deadline*, GAO-15-739 (Washington, DC: GAO, September 2015), <http://www.gao.gov/assets/680/672320.pdf> (accessed August 22, 2020); GAO, *Passenger Rail Security: Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives*, GAO-13-20 (Washington, DC: GAO, December 2012), <http://www.gao.gov/assets/660/650995.pdf> (accessed August 22, 2020).
- 80 DHS, Office of Inspector General, *DHS Grants Used for Mitigating Risk to Amtrak Rail Stations* (Washington, DC: DHS, March 2010), <http://www.documentcloud.org/documents/240714-dhs-grants-used-for-mitigating-risks-to-amtrak.html> (accessed August 22, 2020).
- 81 DHS, DHS announces grant guidance for fiscal year (FY) 2015 preparedness grants, <http://www.dhs.gov/news/2015/04/02/dhs-announces-grant-guidance-fiscal-year-fy-2015-preparedness-grants> (accessed August 22, 2020).
- 82 For a thorough review of its security initiatives, see: Amtrak, *Amtrak Security Measures*, http://media.amtrak.com/wp-content/uploads/2015/10/Security_Fact_Sheet_5-5-16.pdf (accessed August 22, 2020).
- 83 J. B. Reed, Securing dangerous rail shipments, *State Legislatures*, 38 (October/November 2007).
- 84 CSX System Map, <https://www.csx.com/index.cfm/customers/maps/csx-system-map/> (accessed August 22, 2020).
- 85 DHS, Office of Inspector General, *TSA's Preparedness for Mass Transit and Passenger Rail Emergencies* (Washington, DC: DHS, March 2010), 32, https://www.oig.dhs.gov/assets/Mgmt/OIG_10-68_Mar10.pdf (accessed August 22, 2020).

Homeland Security and Public Health

OBJECTIVES

1. To define the various public health challenges in the field of homeland security
2. To outline the various agencies, aside from DHS, that are involved in public health risks
3. To analyze and assess the public health threats that emerge from specified sectors including water, agriculture and food and infectious animals
4. To comprehend the various methods that may be used in an attack on the public water supply
5. To describe how vulnerability assessments are used in the protection of the country's water and food supplies
6. To comprehend the various methods that may be used in an attack on the public food supply
7. To identify the programs in place to protect and test the country's food supply
8. To explain the various infectious and communicable diseases that can be used as tools of terrorism
9. To list the various pandemic threats that may be used in a terror attack
10. To evaluate the impact of the COVID-19 pandemic in relation to our homeland security and defense

11.1 Introduction: Public Health and Homeland Security

At first glance, it seems that public health and homeland security are unrelated in scope and design. Nothing could be farther from the truth, for questions involving public health inexorably wind their way back to issues of safety and security in a host of contexts. The events and circumstances surrounding the recent and ongoing COVID-19 pandemic make clear the fragility of our national interest, our economic system, and the health and safety of the citizenry. COVID-19 may turn out to have worse and greater impact on our homeland security than any other event including the devastation caused by 9/11. See Figure 11.1.¹

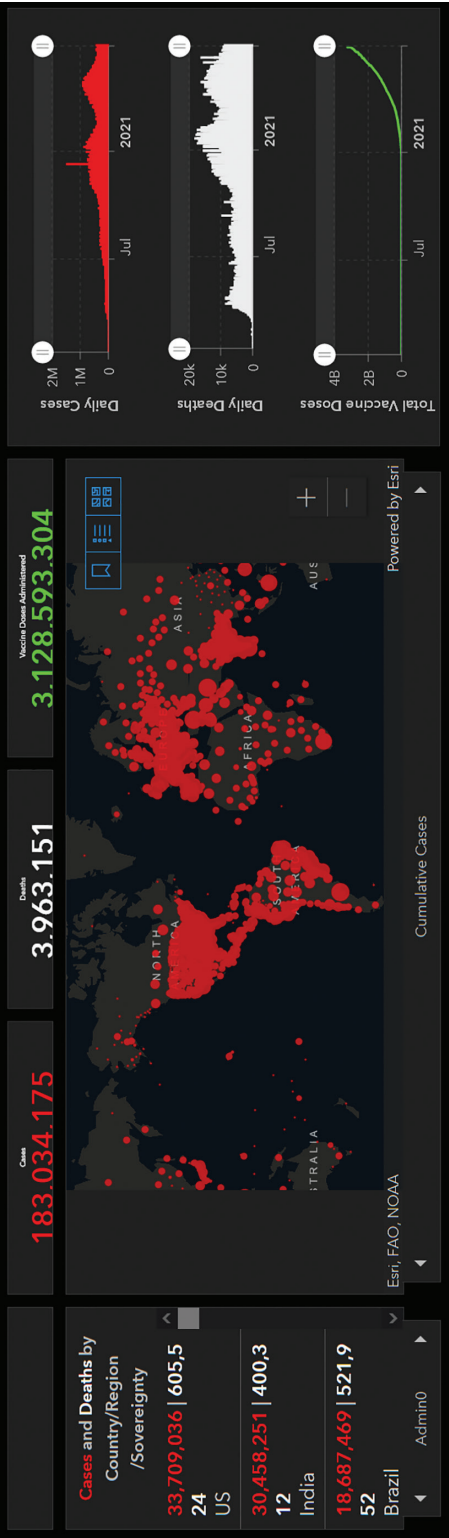


Figure 11.1 Johns Hopkins Map of COVID-19 Cases as of July 2021. (Courtesy of Johns Hopkins University School of Medicine.)

11.1 Introduction: Public Health and Homeland Security

By any reasonable interpretation, health dilemmas, whether infectious, toxic, metabolic, or otherwise, and regardless of intent or national origin can cause significant harm to both individuals and the common good. While public health connotes a host of threats, the spectrum of health issues cannot be fully categorized. For example, the entire world of viruses and biotoxins injures by attacking the physical integrity of the body, undermining the economic and social order and causing social isolation that brings its own costs. The fear of viruses and biotoxins generates extraordinary fear. The very word “anthrax” sends chills into the population just as the pandemic virus wreaks havoc on every aspect of human operations. Pathogens, chemical release agents, and biological and chemical substances, COVID-19 all impact the individual person and community tranquility. Sometimes the fear is worse than the actual harm caused but COVID-19 manifested this cultural paralysis.²

Assaults on the public health can have catastrophic consequences and impact all sectors protected by homeland security policy and practice. The COVID-19 crisis manifests this very negative reality as we have topped over 600,000 dead in the United States alone. Public health threats, like COVID-19 and its natural propensity to undermine homeland security, must not be relegated to medical professionals alone. The Department of Homeland Security (DHS) fully connects public health challenge with the homeland protection. The public health system is one of its 16 critical areas of infrastructure (Boxes 11.1 and 11.2).³ At the same time, public health challenges can emerge in all 16 sectors for homeland security purposes.

Anticipating how the public health challenge might arise in these sectors can be discovered during vulnerability assessments and analyses.

BOX 11.1 VULNERABILITY ASSESSMENT FACTSHEET

WHAT IS THE PURPOSE OF VULNERABILITY ASSESSMENTS

Vulnerability assessments help water systems evaluate susceptibility to potential threats and identify corrective actions that can reduce or mitigate the risk of serious consequences from adversarial actions (e.g., vandalism, insider sabotage, terrorist attack, etc.). Such an assessment for a water system takes into account the vulnerability of the water supply (both ground and surface water), transmission, treatment, and distribution systems. It also considers risks posed to the surrounding community related to attacks on the water system. An effective vulnerability assessment serves as a guide to the water utility by providing a prioritized plan for security upgrades, modifications of operational procedures, and/or policy changes to mitigate the risks and vulnerabilities to the utility's critical assets. The vulnerability assessment provides a framework for developing risk reduction options and associated costs. Water systems should review their vulnerability assessments periodically to account for changing threats or additions to the system to ensure that security objectives are being met. Preferably, a vulnerability assessment is *performance based*, meaning that it evaluates the risk to the water system based on the effectiveness (performance) of existing and planned measures to counteract adversarial actions.

WHAT ARE THE BASIC ELEMENTS OF VULNERABILITY ASSESSMENTS?

The following are common elements of vulnerability assessments. These elements are conceptual in nature and not intended to serve as a detailed methodology.

1. Characterization of the water system, including its mission and objectives
2. Identification and prioritization of adverse consequences to avoid
3. Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences

4. Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries
5. Evaluation of existing countermeasures
6. Analysis of current risk and development of a prioritized plan for risk reduction

The vulnerability assessment process will range in complexity based on the design and operation of the water system itself. The nature and extent of the vulnerability assessment will differ among systems based on a number of factors, including system size, potential population affected, source water, treatment complexity, system infrastructure, and other factors. Security and safety evaluations also vary based on knowledge and types of threats, available security technologies, and applicable local, state, and federal regulations.

BOX 11.2 CRITICAL INFRASTRUCTURE SECTORS

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

PPD-21 identifies 16 critical infrastructure sectors:

Chemical Sector

DHS is designated as the sector-specific agency for the chemical sector.

Commercial Facilities Sector

DHS is designated as the sector-specific agency for the commercial facilities sector.

Communications Sector

The communications sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government.

Critical Manufacturing Sector

DHS is designated as the sector-specific agency for the critical manufacturing sector.

Dams Sector

DHS is designated as the sector-specific agency for the dams sector. The dams sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Defense Industrial Base Sector

The defense industrial base sector is the worldwide industrial complex that enables research and development (R&D), as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

Emergency Services Sector

DHS is designated as the sector-specific agency for the emergency services sector. A system of prevention, preparedness, response, and recovery elements, the emergency services sector represents the nation's first line of defense in the prevention and mitigation of risk from terrorist attacks, manmade incidents, and natural disasters.

Energy Sector

The U.S. energy infrastructure fuels the economy of the twenty-first century. The Department of Energy is the sector-specific agency for the energy sector.

Financial Services Sector

The Department of Treasury is designated as the sector-specific agency for the financial services sector.

Food and Agriculture Sector

The U.S. Department of Agriculture (USDA) and the Department of Health and Human Services (HHS) are designated as the co-sector-specific agencies for the food and agriculture sector.

Government Facilities Sector

DHS and the General Services Administration are designated as the co-sector-specific agencies for the government facilities sector.

Health Care and Public Health Sector

HHS is designated as the sector-specific agency for the health care and public health sector.

Information Technology Sector

DHS is designated as the sector-specific agency for the information technology sector.

Nuclear Reactors, Materials, and Waste Sector

DHS is designated as the sector-specific agency for the nuclear reactors, materials, and waste sector.

Transportation Systems Sector

DHS and the Department of Transportation are designated as the co-sector-specific agencies for the transportation systems sector.

Water and Wastewater Systems Sector

The Environmental Protection Agency (EPA) is designated as the sector-specific agency for the water and wastewater systems sector.

It is not the targeted sector alone that should weigh and assess potential vulnerabilities in public health crisis. Hospitals, labs, pharmaceutical companies, water and energy companies, and a host of aligned facilities all play a key role in the event of an attack on the public health.⁴ DHS is not the sole agency entrusted with this sort of assessment since others need to be involved, such as HHS, the EPA, the Department of Energy, and the Departments of the Interior and Agriculture. While space cannot allow for coverage of each and every element in the health sector, this section will assess the more commonly known homeland—public health connections, commencing with water facilities.

11.2 Water and Public Health

It would be difficult to name a more essential component to physical life than water itself. Treatment plants have been a target of the terrorist, and in a perverse way, successful access to a treatment plant would be a dramatic victory for America's enemies. The EPA assumes the lead role in the protection of our water supply from a public health attack. As in all aspects of traditional American life, 9/11 triggered a new way of looking at water facilities. Soon after 9/11, Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Public Law No: 107-188), which zeroed in on the horrid possibility of water contamination as an act of terror. In Section 402 of the act it states:

Homeland Security

VULNERABILITY ASSESSMENTS—(1) Each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the vulnerability of its system to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. The vulnerability assessment shall include, but not be limited to, a review of pipes and constructed conveyances, physical barriers, water collection, pretreatment, treatment, storage and distribution facilities, electronic, computer or other automated systems which are utilized by the public water system, the use, storage, or handling of various chemicals, and the operation and maintenance of such system. The Administrator, not later than August 1, 2002, after consultation with appropriate departments and agencies of the Federal Government and with State and local governments, shall provide baseline information to community water systems required to conduct vulnerability assessments regarding which kinds of terrorist attacks or other intentional acts are the probable threats to

A. Substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or

B. Otherwise present significant public health concerns.

As part of our critical infrastructure, they become more than water plants but targets for the terrorist. In response to the September 11, 2001, attacks, the EPA formed the Water Security Division (WSD) in the Office of Ground Water and Drinking Water. WSD oversees all drinking water and wastewater homeland security matters. The Office of Homeland Security (OHS) was created in the EPA Office of the Administrator to oversee all EPA matters related to homeland security (Figure 11.2).⁵

Drinking Water Requirements for States and Public Water Systems

CONTACT US
SHARE   

[Drinking Water Requirements Home](#)

[Drinking Water Rules](#)

[Water Supply Guidance](#)

[Training](#)

[Learn about Water Systems](#)

[State Resources](#)

[Water System Resources](#)

[Schools and Child Care Facilities](#)

Information about Public Water Systems

Providing safe drinking water is a partnership that involves EPA, the states, tribes, water systems, and water system operators. The public drinking water systems regulated by EPA and delegated states and tribes provide drinking water to 90 percent of Americans.

A public water system provides water for human consumption through pipes or other constructed conveyances to at least 15 service connections or serves an average of at least 25 people for at least 60 days a year. A public water system may be publicly or privately owned.

There are over 148,000 public water systems in the United States.

EPA classifies these water systems according to the number of people they serve, the source of their water, and whether they serve the same customers year-round or on an occasional basis.

Classifications:

EPA has defined three types of public water systems:

- **Community Water System (CWS):** A public water system that supplies water to the same population year-round.
- **Non-Transient Non-Community Water System (NTNCWS):** A public water system that regularly supplies water to at least 25 of the same people at least six months per year. Some examples are schools, factories, office buildings, and hospitals which have their own water systems.
- **Transient Non-Community Water System (TNCWS):** A public water system that provides water in a place such as a gas station or campground where people do not remain for long periods of time.

Related Information

- [Drinking Water Distribution System](#)
- [Public Water System Supervision Program](#)
- [Private Drinking Water Wells](#)

Figure 11.2 Information about public water systems in the United States. (From EPA, Information about public water systems.)

The WSD tackled a host of issues relating to security and the water supply, and these tasks can be broken down into the following:

- Sector profile and goals
- Identifying assets, systems, networks, and functions
- Assessing risks
- Prioritizing infrastructure
- Developing and implementing protective programs
- Measuring progress
- Protection R&D
- Managing and coordinating responsibilities

Here one witnesses an agency running full steam regarding the question of security and water. The infection of a water supply would be a major health risk and likely cause more casualties than any aircraft flying into a building.⁶ The EPA views threat analysis broadly, encompassing natural events, criminal acts, insider threats, and foreign and domestic terrorism. Natural catastrophic events are typically addressed as part of emergency response and business continuity planning; yet the same skill sets necessary for the planning and mitigation of the terrorist attack on the water supply are needed.

To analyze and prepare for threats and attacks, the agency needs to think of the predictable methods the terrorist would employ. Assessment requires a certain amount of foresight. The oft-cited methodology regarding water facilities usually includes

- Chemical, biological, or radiological (CBR) contamination attacks on drinking water assets, especially distribution systems
- Vehicle-borne improvised explosive devices and improvised explosive device attacks on infrastructure, especially single points of failure and chemical storage sites
- Cyber-attacks on industrial control systems
- Chemical attacks, which may include introduction of a combustible contaminant into a wastewater collection system, affecting infrastructure or the treatment process

Hence, it is risk assessment in all its glory that water facilities have to engage in. The homeland security professional needs to ask questions that anticipate the risk and corresponding plan. At most water facilities, the threats are encompassed in these queries:

- What are the most plausible threats, contaminants, and threat scenarios facing the drinking water industry?
- How does this information compare with intelligence information on possible threats?
- What types of biological and chemical contaminants could be introduced into water systems, and what are their physical, chemical, and biological properties?
- What are the potential health impacts of these contaminants?
- What are the most effective means to destroy contaminants in water?
- How can this information be combined with reporting, analysis, and decision-making to arrive at a reliable system?
- Can effective methods be developed to ensure that a sufficient number of qualified laboratories exist to perform rapid analysis of water contaminants in the event of an attack?
- If contaminants are introduced into a water system, where will they travel?

Homeland Security

- How quickly will they travel?
- What will be their concentration at various points along their path?
- Can human exposures and the health impacts of these contaminants be effectively minimized?
- How can water that has been contaminated be effectively treated so that it can be released to wastewater systems or otherwise disposed of?
- Are alternative water supplies available in the event of an attack?
- How would water utilities or governments most effectively select a cost-effective early warning system?

Any meaningful security plan will anticipate these questions and will prompt the security professional to devise a plan that mitigates the damage and redirects the water facility to positive productivity after this event. Most water facilities need to rely on both internal and external constituencies to fully comprehend the dynamics of their location. The interplay between state and federal regulators alone gives some sense of this necessary interconnection.

Internet Exercise: Find out about the Water Information Sharing and Analysis Center (WaterISAC) professional association of water providers and the security tool made available by this group at <http://www.dhs.gov/critical-infrastructure-sectors>.

Most water facilities engage in a serious self-assessment program that looks to these 14 variables, as published by the EPA:

- Explicit commitment to security
- Promote security awareness
- Defined security roles and employee expectations
- Vulnerability assessment up to date
- Security resources and implementation priorities
- Contamination detection
- Threat-level-based protocols
- Emergency response plan (ERP) tested and up to date
- Utility-specific measures and self-assessment
- Intrusion detection and access control
- Information protection and continuity
- Design and construction standards
- Communications
- Partnerships

To ensure basic compliance with these criteria, the water facility should conduct its own vulnerability assessment. The EPA, as well as a host of software companies, makes available vulnerability assessment programs. The EPA publishes vulnerability and assessment guidelines, which are reproduced in the following section (Figure 11.3).⁷

Internet Exercise: Learn how to prepare for flooding's impact on the water supply at <http://www.epa.gov/sites/production/files/2015-06/documents/flooding.pdf>.

RISK AND RESILIENCE ASSESSMENTS AND EMERGENCY RESPONSE PLANS.

NEW REQUIREMENTS FOR DRINKING WATER UTILITIES

Section 2013 of America's Water Infrastructure Act of 2018 (AWIA) requires community water systems¹ that serve more than 3,300 people to complete a risk and resilience assessment and develop an emergency response plan.

	RISK AND RESILIENCE ASSESSMENT	EMERGENCY RESPONSE PLAN
Important Dates	Your utility must conduct a risk and resilience assessment and submit certification of its completion to the U.S. EPA by the following dates: ● March 31, 2020 if serving ≥100,000 people. ● December 31, 2020 if serving 50,000 to 99,999 people. ● June 30, 2021 if serving 3,301 to 49,999 people.	Your utility must develop or update an emergency response plan and certify completion to the U.S. EPA no later than six months after risk and resilience assessment certification. Each utility deadline is unique; however, the dates below are the due dates for utilities who submit a risk and resilience assessment certification by the final due date according to the population served. ● September 30, 2020 if serving ≥100,000 people. ● June 30, 2021 if serving 50,000 to 99,999 people. ● December 30, 2021 if serving 3,301 to 49,999 people.
Recertification	Every five years, your utility must review the risk and resilience assessment and submit a recertification to the U.S. EPA that the assessment has been reviewed and, if necessary, revised. Visit the U.S. EPA website to find more information on guidance for developing a risk and resilience assessment at https://www.epa.gov/waterriskassessment/conduct-drinking-water-or-wastewater-utility-risk-assessment.	Within six months of submitting the recertification for the risk and resilience assessment, your utility must certify it has reviewed and, if necessary, revised, its emergency response plan. Visit the U.S. EPA website for guidance on developing an Emergency Response Plan at https://www.epa.gov/waterutilityresponse/develop-or-update-drinking-water-or-wastewater-utility-emergency-response-plan.

TOOLS OR METHODS

AWIA does not require the use of any standards, methods or tools for the risk and resilience assessment or emergency response plan. Your utility is responsible for ensuring that the risk and resilience assessment and emergency response plan address all the criteria in AWIA Section 2013(a) and (b), respectively. The U.S. EPA recommends the use of standards, including AWWA J100-10 Risk and Resilience Management of Water and Wastewater Systems, along with tools from the U.S. EPA and other organizations, to facilitate sound risk and resilience assessments and emergency response plans.

¹ Section 2013 of AWIA applies to community water systems. Community water systems are drinking water utilities that consistently serve at least 25 people or 15 service connections year-round.

Still have questions about the new AWIA requirements?
Contact the U.S. Environmental Protection Agency (U.S. EPA) at dwwresilience@epa.gov.

Office of Water (4608T)
EPA-817-F-19-004
May 2019

Figure 11.3 EPA water risk, resilience assessment, and response plan.

11.3 Agriculture, Food, and Public Health

Just as water contamination has enormous impacts on the public health of the nation, so too does the integrity of its food supply. Here again, the terrorist envisions a target that has widespread potential for harm to a significant portion of the population.⁸ Agriculture and food systems are vulnerable to disease, pests, or poisonous agents that occur naturally, are unintentionally

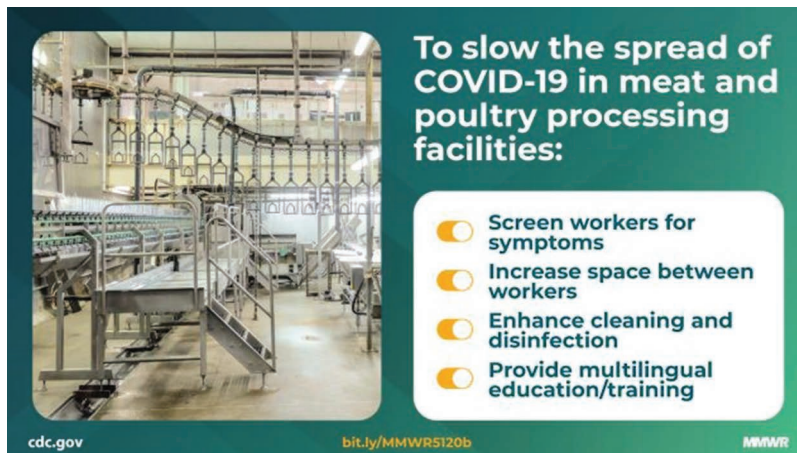


Figure 11.4 Meat packing plant COVID-19 safety guidelines from the CDC.

introduced, or are intentionally delivered by acts of terrorism. Food supply can surely be impacted by public health crises as well. Throughout the COVID-19 pandemic, the continued flow of agricultural products has been a constant DHS concern.⁹ In some cases, meat processing plants became epicenters for the virus due to close quarters and fast spread possible in the industry. The Centers for Disease Control (CDC) has issued guidance on how to minimize the COVID virus in these facilities. See Figure 11.4.¹⁰

The challenges of assuring a safe environment in meat processing plants have been dramatically apparent in both the number of infections and the measures recommended to alter the spread. Table 11.1¹¹ lays out the consensus recommendations on how to assure a safe, stable, and productive meat facility.

Food can be attacked on many fronts, including:

- Biological and chemical agents
- Naturally occurring, antibiotic-resistant, and genetically engineered substances
- Deadly agents and those tending to cause gastrointestinal discomfort
- Highly infectious agents and those that are not communicable
- Substances readily available to any individual and those that are more difficult to acquire
- Agents that must be weaponized and those that are accessible in a usable form¹²

America's agriculture and food system is an extensive, open, interconnected, diverse, and complex structure, and, as a result, the perfect forum for the terrorist.

Responsibility for the food supply, from a security perspective, resides in three government agencies: the USDA, the Food and Drug Administration (FDA), and DHS. In a recent report, these agencies set out a vision statement on the food supply (Figure 11.5).¹³

As appropriate, the USDA takes the lead role in the protection of our food supply. As it notes, "The protection and integrity of America's agricultural production and food supply are essential to the health and welfare of both the domestic population and the global community"¹⁴ (Figure 11.6).

Internet Exercise: The list of food recalls due to safety and health questions will be surprising. Visit http://www.fsis.usda.gov/FSIS_Recalls/Recall_Case_Archive/index.asp.

The impact of food and agriculture contamination is not lost on DHS. Its recommendations on the integrity of the food chain are incisive, asking those entrusted with its safety to truly

Table 11.1 Detailed Guidelines on COVID-19 Safety for Meat Packing Facilities^a

Category	Challenges to Effective Prevention and Control of COVID-19	Recommended Changes in Facility Practice ^b
Structural	Maintaining physical distancing during breaks and when employees enter and exit the facility	Adjust start and stop times of breaks and shifts Add outdoor breakrooms
	Maintaining physical distancing on production line	Install physical barriers between workers
	Excluding symptomatic workers	Screen all workers and visitors entering facility and plan for effective isolation for workers who become ill at work
Operational	Maintaining physical distancing on production line	Reduce rate of animal processing
	Adhering to face covering recommendations	Require universal face covering Ensure face coverings conformed to CDC guidance Provide training on donning and doffing
	Adhering to heightened cleaning and disinfection guidelines	Assign additional staff to sanitize “high touch” areas (e.g., handles, buttons, railings) more frequently Add several hand sanitizer dispensers and handwashing stations implement touch-free time clocks
Sociocultural	Communicating through language and cultural barriers	Engage community partners to develop culturally informed messaging Disseminate messaging in languages spoken among the work force
	Employees live in crowded, multigenerational settings	Include messaging about behaviors employees should take to limit the spread of the virus while at home
	Employees share transportation to and from work	Add additional vehicles to shuttle routes Require use of face coverings during commute
Economic	Employees incentivized to work while ill	Implement personnel policies that provide additional medical leave and disability benefits without loss of seniority or pay Remove financial incentives, such as attendance bonuses

COVID-19, coronavirus disease 2019.

^a Based on CDC field team deployments to tour sites and information gathered from calls with state health departments.

^b Based on on-site and remote technical assistance, many facilities have implemented or are planning to implement these strategies.

Homeland Security

Vision and Purpose of DHS: Food and Agricultural Section

The FA Sector comprises complex production, processing, and delivery systems. The mission of the FA Sector is to protect against a disruption in the food supply that would pose a serious threat to public health, safety, welfare, or to the national economy. These food and agriculture systems are almost entirely under private ownership, and they operate in highly competitive global markets, strive to operate in harmony with the environment, and provide economic opportunities and an improved quality of life for U.S. citizens and others worldwide.

Differences in commodity type, farm size, operator, and household characteristics complicate prevention and protection efforts for individual operations and, ultimately, the sector as a whole. In recent years, changes in the rules of trade, shifts in domestic policy, and new developments in technology have altered the competitive landscape of global agriculture and challenges facing American farmers.

Securing this sector presents unique challenges because food and agriculture systems in the United States are extensive, open, interconnected, and diverse, and they have complex structures. Food products move rapidly in commerce to consumers, but the time required for detection and identification of attacks and contaminations, such as animal or plant disease introduction or food contamination, can be lengthy and complex. Therefore, attacks and contaminations on the FA Sector could result in severe animal, plant, public health, and economic consequences.

Figure 11.5 Vision statement for the food and agriculture sector. (From DHS, Food and Agriculture Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan (2010).)



Figure 11.6 A Midwestern farm.

consider the ramifications of contamination. DHS poses seven criteria for consideration when weighing the impact of food contamination.

Criticality: What will be the public health impacts and economic costs associated with the attack?

Accessibility: How easy will it be for a terrorist to gain access and egress from the location of the food and agricultural product?

Recuperability: How readily will the food supply system recover from an attack?

Vulnerability: How easy or difficult will the attack be?

Effect: What calculable losses will there be directly resulting from the attack?

Recognizability: Are targets easy to discover and identify?

Shock: In a cumulative sense, how significant are the health, economic, and psychological impacts that result from the attack?¹⁵

In each of these categories, the ramifications of a food contamination event are obvious. As in the water supply, the far-reaching impacts of food contamination are almost impossible to measure. Yet those entrusted with production must be mindful of their product's safety and security as well. Whether it is grain or cattle, soybeans or chicken, the agricultural entrepreneur must tend to questions on security daily.

Determining exactly how to ensure security in the agricultural sphere is no simple undertaking. Aside from the broad range of products and services, there is the added dilemma of multiple agency responsibility. While the USDA may be at the forefront, its policymaking on food and its safety is influenced by myriad other agencies, such as the FDA and EPA, and its own internal history has protocols and programs that have historically dealt with food safety. In this area, it is clear that many adjustments and realignments have had to take place—some readily and others with the usual bureaucratic resistance. Figure 11.7 demonstrates the levels of participation already evident in the USDA prior to and after 9/11.

Meshing all of this historic practice into a unified and seamless vision of security in light of 9/11 is a challenging undertaking. What emerges from the USDA is an agency in full recognition of this challenge. It urges its constituency to conduct risk assessments, to realize that security questions are central to farm operation, and to accept some level of personal responsibility for the integrity of facility and product.

USDA mission area	Agency
Farm and foreign agriculture services	• Farm service agency (FSA) • Foreign agricultural service (FAS) • Risk management agency (RMA)
Food, nutrition, and consumer services	• Center for nutrition policy and promotion (CNPP) • Food and nutrition service (FNS)
Food safety	• Food safety and inspection service (FSIS)
Natural resources and environment	• Forest service (FS) • Natural resources conservation service (NRCS)

Figure 11.7 USDA's participation in homeland security. (From USDA, DHS, and FDA, *Critical Infrastructure and Key Resources for Sector Specific Plan as Input to the National Infrastructure Protection Plan* (Washington, DC: U.S. Government Printing Office, 2007), 15.)

Homeland Security

In fact, the USDA fully integrates the functions of homeland security into its very makeup, as evidenced by its organizational chart in Figure 11.8.

The USDA calls on all owners in the agricultural sector to view security in both general and specific product terms. In the more general arena, it recommends the following assessment protocol:

- Procedures are in place for notifying appropriate law enforcement when a security threat is received, or when evidence of actual product tampering is observed.
- Procedures are in place for heightened awareness (especially when the DHS terrorism threat level is elevated) for unusual activities around the farm and increased disease symptoms among animals or crops.
- A current local, state, and federal government Homeland Security contact is maintained.
- All employees are encouraged to report any sign of product tampering.
- Facility boundaries are secured to prevent unauthorized entry.
- “No Trespassing” and “Restricted Entry” signs are posted appropriately.
- Alarms, motion detection lights, cameras, and other appropriate security equipment are used in key areas, as needed.
- Facility perimeter is regularly monitored for signs of suspicious activity or unauthorized entry.
- Doors, windows, gates, roof openings, vent openings, trailer bodies, railcars, and bulk storage tanks are secured at all times.
- Outside lighting is sufficient to allow detection of unusual activities.
- Fire, smoke, and heat detection devices are operable throughout the farm.
- Storage tanks for hazardous materials and potable water supply are protected from, and monitored for, unauthorized access.

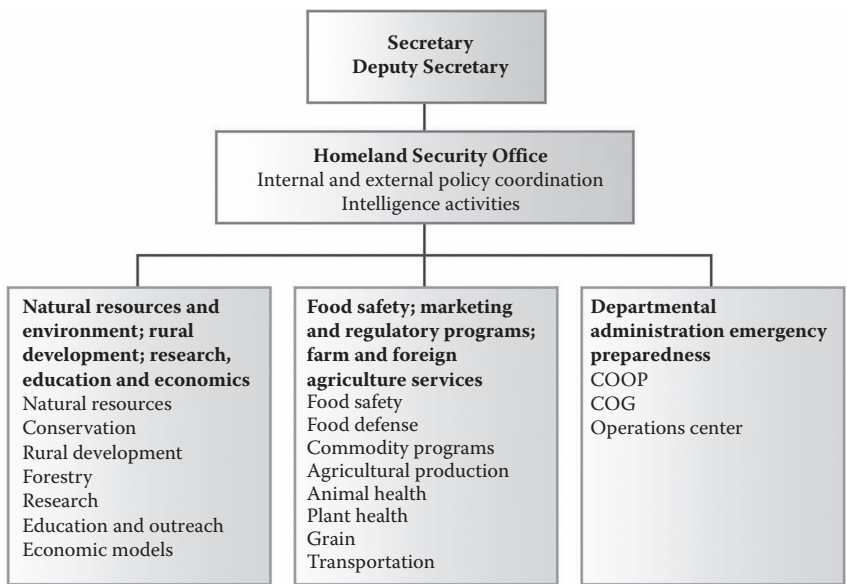


Figure 11.8 USDA structure for homeland protection and food safety. (From USDA, DHS, and FDA, *Critical Infrastructure*, 36.)

- Wells and other water supplies are secured and routine testing is performed.
- Truck deliveries are verified against a roster of scheduled deliveries.
- Unscheduled deliveries are held away from facility premises pending verification of shipper and cargo.
- Records are maintained for all vehicles and equipment: make, model, serial number, service date, and so on.
- Vehicles and equipment are secured or immobilized when not in use; keys are never left in unattended vehicles.
- Machinery is removed from fields and stored appropriately; valuable equipment and tools are locked in a secure building.
- Entry into facility is controlled by requiring positive identification (i.e., picture ID).
- New employees are screened and references are checked.
- Visitors and guests are restricted to nonproduction areas unless accompanied by a facility employee.
- Where required by biosecurity procedures, visitors wear clean boots or coveralls (disposable boots and coveralls are provided for visitors).
- Areas are designated for check-in and check-out for visitors/deliveries (with a sign-in sheet for name, address, phone number, reason for visit).
- An inspection for signs of tampering or unauthorized entry is performed for all storage facilities regularly.
- Hazardous materials are purchased only from licensed dealers.
- A current inventory of hazardous or flammable chemicals (including drugs, chemicals, pesticides, and fertilizers) or other products (including chemical trade names, product type, EPA numbers, quantity, and usage) is maintained, and discrepancies are investigated immediately.
- A current inventory of stored fuel (diesel, gasoline, fuel oil, propane, oxygen, acetylene, kerosene, etc.) is maintained.
- A disease surveillance plan is available.
- Risk management plans have been developed or updated and shared with employees, family, visitors, customers, and local law enforcement.
- Plans include awareness of animal and plant health, as well as signs of tampering with crops, livestock, supplies, vehicles, equipment, and facilities.
- Orientation/training on security procedures is given to all facility employees at least annually.
- Passwords for USDA systems and programs are protected to prevent unauthorized user entry.¹⁶

11.3.1 Strategic Partnership Program on Agroterrorism

Attacks against the agricultural system would be an effective and frightful way of inflicting a terrorist act, and law enforcement needs to anticipate the possibility. “Agroterrorism has been defined as the deliberate introduction of an animal or plant disease with the goal of generating fear, causing economic losses or undermining social stability.”¹⁷ Knowledge about food supply resides in a bevy of private and public entities and will require a major collaboration.

Homeland Security

Blending diverse agencies with distinct approaches to security has been a challenge for those protecting the food supply. Put another way, law enforcement officials, such as the FBI or Customs, will see the food problem through a prism of enforcement, while food safety specialists at the USDA or FDA may see things from a different perspective. The Strategic Partnership Program on Agroterrorism (SPPA) makes a noble effort to meld these various visions and to unify these diverse perspectives into one framework—that of food safety. Just as critically, the SPPA will enlist private industry concerns, from farmers to grain processors, from stockyard owners to fertilizer companies. The objectives of the SPPA are as follows:

- Validate or identify sector-wide vulnerabilities by conducting critical infrastructure/key resources (CI/KR) assessments in order to
 - Identify gaps.
 - Inform Centers of Excellence and Sector Specific Agencies (SSA) of identified research needs.
 - Catalog lessons learned.
- Identify indicators and warnings that could signify planning for an attack.
- Develop mitigation strategies to reduce the threat/prevent an attack. Strategies may include actions that either industry or government may take to reduce vulnerabilities.
- Validate assessments conducted by the United States Government (USG) for food and agriculture sectors.
- Gather information to enhance existing tools that both USG and industry employ.
- Provide the USG and the industry with comprehensive reports including warnings and indicators, key vulnerabilities, and potential mitigation strategies.
- Provide subsector reports for the USG that combines assessment results to determine national critical infrastructure vulnerability points to support the National Infrastructure Protection Plan (NIPP) and national preparedness goals.
- Establish and/or strengthen relationships between federal, state, and local law enforcement and the food and agriculture industry along with the critical food/agriculture sites visited.¹⁸

SPPA relies on industry visitations to reach its conclusions about safety and security in the agricultural sector. This is why private industry—namely, farmers and food suppliers—is so integral to the SPPA process. SPPA assessments are conducted on a voluntary basis between one or more industry representatives for a particular product or commodity. As recommended by DHS and the USDA, industry production processes are evaluated in light of law enforcement officials. Together, they conduct a vulnerability assessment using the seven criteria noted previously: criticality, accessibility, recuperability, vulnerability, effect, recognizability, and shock.

As a result of each assessment, participants identify weaknesses in the production cycle as well as recommendations on protective measures and mitigation steps that may reduce the vulnerability. By 2012, both actual and proposed new assessments shown in Table 11.2¹⁹ had been conducted or soon to be conducted under the SPPA program.

Proposed future inspections, conducted by the USDA and the FDA, will tackle a host of foodstuffs and agricultural products including those shown in Table 11.3.²⁰

Internet Exercise: For full instructions on how to devise a food safety program, see http://www.fsis.usda.gov/PDF/Food_Defense_Plan.pdf.

The USDA's Food Safety and Inspection Service (FSIS) has developed a surveillance program to randomly screen and check food facilities as well as be stationed at ports of entry. Food safety officers are a sought-after career track due to the excellent working conditions and challenging work. FSIS continues to hire import surveillance liaison officers who are responsible for the

Table 11.2 New Assessments

Product/Process	Assessment Date	Location	Trade Association
Restaurants	10/6/2009	Woodrow Wilson Service Area, NJ Turnpike	New Jersey Restaurant Association
Coffee shops	10/7/2009	Woodrow Wilson Service Area, NJ Turnpike	New Jersey Restaurant Association
Pet food	10/16/2009	Washington, DC	Pet Food Institute
Animal by-products	12/1/2009	Arlington, VA	National Renderers Association
Baked goods	1/15/2010	Arlington, VA	American Bakers Association
Ice cream	3/31/2010	Arlington, VA	International Dairy Foods Association
Breaded fish products	4/22–23/2010	Arlington, VA	National Fisheries Institute
Ready to eat seafood (surimi)	7/29/2010	Arlington, VA	National Fisheries Institute
Deli-salads	5/6/2010	Atlanta, GA	NA
Imported product: spices	5/18/2010	Arlington, VA	American Spice Trade Association
Chocolate: candy bar	10/7/2010	Washington, DC	National Confectioners Association
Milk transportation	1/18/2011	Arlington, VA	International Dairy Foods Association
Orange juice storage and transportation	1/12/2011	Arlington, VA	Juice Products Association
Canned tuna	4/28–29/2011	Hat Yai, Thailand	NA
Retail/distribution	5/3–4/2011	Bangkok, Thailand	NA
Rice	5/6–7/2011	Chiang Mai, Thailand	NA
Canned fruit	4/25–26/2011	Kasetsart, Thailand	NA
Catering	10/5/2011	Arlington, VA	International Association of Venue Managers

agency's oversight of food defense issues relating to imported food products at ports of entry, at border entries, and in commerce around the country. In particular, they have expanded their liaison activities with DHS's Customs and Border Protection.

Internet Exercise: To learn about jobs in food safety, see <https://www.fsis.usda.gov/wps/portal/fsis/topics/careers/opportunities-and-types-of-jobs/food-inspector-and-consumer-safety-inspector>.

Table 11.3 Update Assessments

General Industry	Update Assessment Date	Location	Original Assessment Date(s)	Original Assessment Location(s)
Feed mill	9/8/2009	Arlington, VA	June 2007	Indiana
Grocery store	10/14/2009	Arlington, VA	August 2007	Pennsylvania
Retail milk	10/15/2009	Arlington, VA	January 2007	Texas
Frozen food	10/22/2009	Arlington, VA	March 2006	Wisconsin/ Florida
High fructose corn syrup	10/29/2009	Arlington, VA	September 2007	Alabama
Infant formula	12/2/2009	Arlington, VA	June 2006	Arizona
Fresh produce	11/17/2009	Arlington, VA	May 2006	California
Distribution centers	11/17/2009	Arlington, VA	November 2007	Virginia
Dry breakfast cereal	12/1/2009	Arlington, VA	July 2007	Minnesota
Baby food	12/1/2009	Arlington, VA	February 2006	Michigan
Bottle water	12/9/2009	Arlington, VA	January 2006	New Jersey
Dairy (fluid milk)	3/30/2010	Arlington, VA	July 2006	New York
Apple juice	5/19/2010	Arlington, VA	April 2006	New Hampshire
Yogurt	6/4/2010	Bloomington, MN	November 2005	Tennessee/ Minnesota
Grain	6/11/2010	Arlington, VA	November 2006	Illinois
Concession-stadium	10/4/2011	Arlington, VA	March 2007	Kansas

11.3.2 Infectious Animals

Animals can be efficient carriers of illness, catastrophic pathogens, and other threats to public health. Recent cases of mad cow disease heighten the impact of disease on public health integrity. Avian flu (AI), swine flu, and rabies are other examples of well-publicized cases. “Direct disease threats to livestock have been seen domestically and internationally. They come in the form of foot and mouth disease (FMD), bovine spongiform encephalopathy (BCE), various animal flues and parasites.”²¹ The USDA has long recognized the meaningful nature of these threats and correlates how they can relate to the problem of homeland security. Working hand in hand with DHS, the USDA, by and through its Agricultural Research Service (ARS), conducts extensive research on animal diseases and their potential for catastrophic consequences. The Plum Island Animal Disease Center is one of the major centers where this form of analysis is conducted (Figure 11.9).



Figure 11.9 Plum Island Animal Disease Center.

The Plum Island facility conducts high-level animal research under the following mission:

Since 1954, the Plum Island Animal Disease Center (PIADC) has served as the front line of the nation's defense against diseases that could devastate markets for livestock, meat, milk, and other animal products. PIADC is the only laboratory in the nation that can conduct initial diagnostic testing for foot-and-mouth disease (FMD). The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service (APHIS) provides this service and develops novel diagnostic tools. In addition, APHIS conducts training for federal and state veterinarians who serve as the first responders in a potential outbreak of a foreign animal disease (FAD). The USDA's Agricultural Research Service (ARS) conducts research on high-consequence FADs at PIADC and develops diagnostic tools, vaccines, and other means for preventing FADs. The Department of Homeland Security's (DHS) Science and Technology Directorate takes vaccines developed by ARS, academia, and industry through the regulatory process to develop and license new vaccines and diagnostics for high-threat FADs.²²

See Figure 11.10.



Figure 11.10 The Plum Island Animal Disease Center (PIADC) logo.

In the northeast corner of the United States, ARS is conducting a myriad of research undertakings at the following facilities:

Washington, DC

- National Arboretum

Newark, DE

- Beneficial Insects Introduction Research

Boston, MA

- Jean Mayer Human Nutrition Research Center on Aging

Beltsville, MD

- Beltsville Human Nutrition Research Center
- Beltsville Agricultural Research Center

Fort Detrick, MD

- Foreign Disease-Weed Science Research

Orono, ME

- New England Plant, Soil and Water Research Laboratory
- National Cold Water Marine Aquaculture Center

Geneva, NY

- Plant Genetic Resources Research
- Grape Genetics Research

Ithaca, NY

- Robert W. Holley Center for Agriculture & Health

Orient Point, NY

- Plum Island Animal Disease Center

University Park, PA

- Pasture Systems & Watershed Management Research



Figure 11.11 APHIS logo.

Wyndmoor, PA

- Eastern Regional Research Center

Kearneysville, WV

- Appalachian Fruit Research Laboratory

Leetown, WV

- Cool and Cold Water Aquaculture Research²³

Working in consort with these facilities is the Animal and Plant Health Inspection Service (APHIS) of the USDA. APHIS performs a host of functions to ensure the safety of animals and the containment of infectious diseases. And with new and virulent strains of viruses, it is all the more important to contain the spread. For example, the Newcastle Virus attacks poultry with ferocity and APHIS is on the forefront at deterring its spread.²⁴

At airport terminals, seaports, and border stations, officers inspect international conveyances and the baggage of passengers for plant and animal products that could harbor pests or disease organisms. At international airports, detector dogs in APHIS's Beagle Brigade help find prohibited agricultural materials. Officers also inspect ship and air cargoes, rail and truck freight, and package mail from foreign countries. At animal import centers, APHIS veterinarians check animals in quarantine. Overseas, APHIS operates preclearance programs to eliminate pests in some imported products right at the source (Figure 11.11).

For a list of some job opportunities at APHIS, review their careers Web page in Figure 11.12.

11.3.3 Infectious Diseases, Bioterrorism, and Public Health

The idea that disease can be an agent of the terrorist is not new.²⁵ In World War I, mustard gas and other virulent gases were used on the battlefield. In Saddam Hussein's Iraq, he thought so little of the Kurds that he used biological agents on them. Anthrax cases have been in the headlines in the last decade. The release of dangerous pathogens and disease-borne agents has allegedly occurred on the battlefield in certain nations, though we have yet to see a full-scale terrorist attack using these agents (Figure 11.13).²⁶

The list of communicable diseases contains a full range of conditions that need reporting to local, state, and federal health authorities. DHS, HHS, and other agencies mandate the reporting of any case that makes the list of diseases (Table 11.4).²⁷ The list of communicable diseases is


United States Department of Agriculture
 Animal and Plant Health Inspection Service

[About APHIS](#) | [Ask The Expert](#) | [Careers](#) | [Contact Us](#) | [Help](#)

[Home](#) | [Our Focus](#) | [Resources](#) | [Newsroom](#) | [Blog](#)

Careers

[Opportunities for Students](#)

[New Employee Orientation](#)

Career Opportunities

Last Modified: Aug 20, 2015

Positions in APHIS

The results of this job search will be compiled specifically for the Animal and Plant Health Inspection Service. Some of the jobs displayed may be restricted to agency and/or department employees only. Please be sure to review the job entries and announcements carefully. Applications from outside of the area of consideration may not be evaluated or acknowledged.

- Veterinary Services Job Openings

Veteran Opportunities

Details and provisions pertaining to the Vow to Hire Heroes Act of 2011.

USDA Pathways Programs

The U.S. Department of Agriculture offers different pathway opportunities for students and recent graduates to work in the agricultural, science, technology, math, environmental, management, business and many other fields. USDA offers internships to students and recent graduates to help them to excel in their chosen fields.

- Opportunities for Students
- USAJobs Students and Grads

Search for positions within the U.S. Government

USAJOBS is the official job site of the US Federal Government. It's your one-stop source for Federal jobs and employment information.

U.S. Office of Personnel Management

The Office of Personnel Management provides valuable employment, pay and performance, and leadership and individual development information for current Federal employees and those looking to work for the Federal Government.

Figure 11.12 APHIS careers Web page. (From U.S. Department of Agriculture. Animal and Plant Health Inspection Service. Career opportunities. <https://www.aphis.usda.gov/aphis/banner/careers.>)

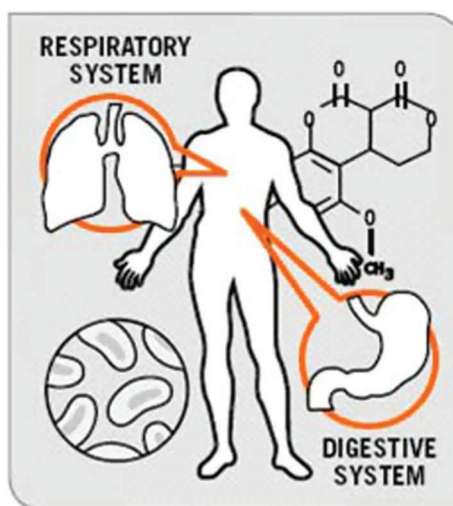


Figure 11.13 Biological attack effects on the major systems of the human body. A biological attack is the release of germs or other biological substances. Many agents must be inhaled, enter through a cut in the skin, or be eaten to make you sick. Some biological agents can cause contagious diseases; others do not.

Table 11.4 List of Reportable Communicable Diseases, 2020

- Anthrax
- Arboviral diseases, neuroinvasive and non-neuroinvasive
 - California serogroup virus diseases
 - Chikungunya virus disease
 - Eastern equine encephalitis virus disease
 - Powassan virus disease
 - St. Louis encephalitis virus disease
 - West Nile virus disease
 - Western equine encephalitis virus disease
- Babesiosis
- Botulism
 - Botulism, foodborne
 - Botulism, infant
 - Botulism, wound
 - Botulism, other
- Brucellosis
- Campylobacteriosis
- *Candida auris*, clinical
- Carbapenemase Producing Carbapenem-Resistant Enterobacteriaceae (CP-CRE)
 - CP-CRE, *Enterobacter* spp.
 - CP-CRE, *Escherichia coli* (*E. coli*)
 - CP-CRE, *Klebsiella* spp.
- Chancroid
- *Chlamydia trachomatis* infection
- Cholera
- Coccidioidomycosis
- Congenital syphilis
 - Syphilitic stillbirth
- Coronavirus disease 2019 (COVID-19)
- Cryptosporidiosis
- Cyclosporiasis
- Dengue virus infections
 - Dengue
 - Dengue-like illness
 - Severe dengue
- Diphtheria
- Ehrlichiosis and anaplasmosis
 - *Anaplasma phagocytophilum* infection
 - *Ehrlichia chaffeensis* infection
 - *Ehrlichia ewingii* infection
 - Undetermined human ehrlichiosis/anaplasmosis
- Giardiasis
- Gonorrhea
- *Haemophilus influenzae*, invasive disease
- Hansen's disease
- Hantavirus infection, non-Hantavirus pulmonary syndrome
- Hantavirus pulmonary syndrome
- Hemolytic uremic syndrome, post-diarrheal
- Hepatitis A, acute
- Hepatitis B, acute

(Continued)

Table 11.4 (Continued) List of Reportable Communicable Diseases, 2020

- Hepatitis B, chronic
- Hepatitis B, perinatal virus infection
- Hepatitis C, acute
- Hepatitis C, chronic
- Hepatitis C, perinatal infection
- HIV infection (AIDS has been reclassified as HIV Stage III)
- Influenza-associated pediatric mortality
- Invasive pneumococcal disease
- Legionellosis
- Leptospirosis
- Listeriosis
- Lyme disease
- Malaria
- Measles
- Meningococcal disease
- Mumps
- Novel influenza A virus infections
- Pertussis
- Plague
- Poliomyelitis, paralytic
- Poliovirus infection, nonparalytic
- Psittacosis
- Q fever
 - Q fever, acute
 - Q fever, chronic
- Rabies, animal
- Rabies, human
- Rubella
- Rubella, congenital syndrome
- *Salmonella Paratyphi* infection (*Salmonella enterica* serotypes Paratyphi A, B [tartrate negative], and C [*S. Paratyphi*])
- *Salmonella typhi* infection (*Salmonella enterica* serotype Typhi)
- Salmonellosis
- Severe acute respiratory syndrome-associated coronavirus disease
- Shiga toxin-producing *Escherichia coli*
- Shigellosis
- Smallpox
- Spotted fever rickettsiosis
- Streptococcal toxic shock syndrome
- Syphilis
 - Syphilis, primary
 - Syphilis, secondary
 - Syphilis, early non-primary non-secondary
 - Syphilis, unknown duration or late
- Tetanus
- Toxic shock syndrome (other than streptococcal)
- Trichinellosis
- Tuberculosis

(Continued)

Table 11.4 (Continued) List of Reportable Communicable Diseases, 2020

- Tularemia
- Vancomycin-intermediate *Staphylococcus aureus* and Vancomycin-resistant *Staphylococcus aureus*
- Varicella
- Varicella deaths
- Vibriosis
- Viral hemorrhagic fever
 - Crimean-Congo hemorrhagic fever virus
 - Ebola virus
 - Lassa virus
 - Lujo virus
 - Marburg virus
 - New World arenavirus —Guanarito virus
 - New World arenavirus—Junin virus
 - New World arenavirus —Machupo virus
 - New World arenavirus—Sabia virus
- Yellow fever
- Zika virus disease and Zika virus infection
 - Zika virus disease, congenital
 - Zika virus disease, non-congenital
 - Zika virus infection, congenital
 - Zika virus infection, non-congenital

Source: CDC, 2016 nationally notifiable infectious diseases, <http://wwwn.cdc.gov/nndss/conditions/notifiable/2020/infectious-diseases>, (accessed August 22, 2020).

regularly updated by both the Centers for Disease Control and Prevention (CDC) and various state health departments.

For those entrusted with security, the problem of disease generally comes in the form of biological agents used in terror attacks. Hence, the term *bioterrorism* has become part of the security vocabulary.²⁸ The CDC defines bioterrorism as an attack involving a

deliberate release of viruses, bacteria, or other germs (agents) used to cause illness or death in people, animals, or plants. These agents are typically found in nature, but it is possible that they could be changed to increase their ability to cause disease, make them resistant to current medicines, or to increase their ability to be spread into the environment. Biological agents can be spread through the air, through water, or in food. Terrorists may use biological agents because they can be extremely difficult to detect and do not cause illness for several hours to several days. Some bioterrorism agents, like the smallpox virus, can be spread from person to person and some, like Anthrax, cannot.²⁹

The CDC tracks and publishes data on the more pressing agents, such as anthrax (Figure 11.14).

Internet Exercise: For the HHS-recommended protocol for countermeasures for bioterrorism, see <http://emergency.cdc.gov/bioterrorism/prep.asp>.

For DHS and HHS, and their collegial partners both governmental and private, the world of bioterrorism is front and center. At the DHS level, bioterrorism will involve three fronts:

- *Infrastructure:* Strengthen health systems, enhance medical communications, and maximize their contribution to the overall biodefense of the nation.
- *Response:* Improve specialized federal capabilities to respond in coordination with state and local governments.
- *Science:* Meet the medical needs of our bioterrorism response plans by developing specific new vaccines, medicines, and diagnostic tests (Figure 11.15). Develop an early warning system for bioterrorism.

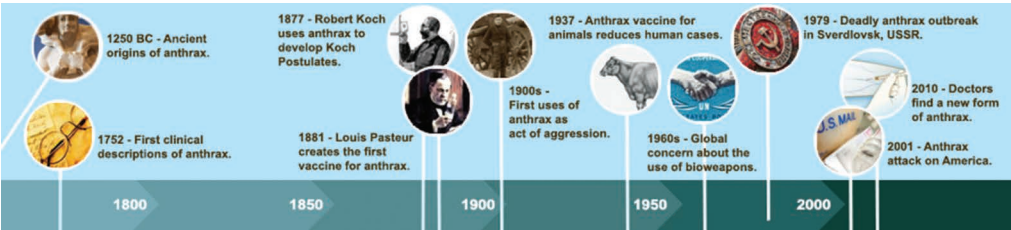


Figure 11.14 Anthrax timeline. (From CDC, Anthrax timeline, <http://www.cdc.gov/anthrax/images/anthrax-timeline.jpg>.)

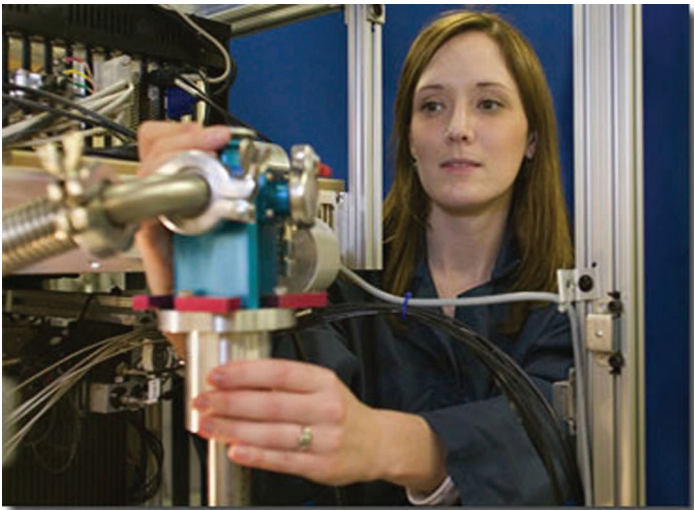


Figure 11.15 HHS chemist.

In the area of infrastructure, both DHS and HHS stress the need for hospital facilities to be in a proactive and reactive capacity when bioterrorism strikes. HHS has devised the Hospital Preparedness Program (HPP), which seeks to elevate the capacity of hospitals to handle public health problems and to prepare for and respond to bioterrorism and other public health emergencies. Priority areas include interoperable communication systems, bed tracking, personnel management, fatality management planning, and hospital evacuation planning. During the last decade, HPP funds have also improved bed and personnel surge capacity, decontamination capabilities, isolation capacity, pharmaceutical supplies, training, education, and drills and exercises.

Internet Exercise: The CDC has provided millions for the critical analysis of COVID-19 research. See <https://www.cdc.gov/grants/public-health-emergencies/covid-19/index.html>.

Hospitals, outpatient facilities, health centers, poison control centers, EMS, and other health-care partners work with the appropriate state or local health department to acquire funding and develop health-care system preparedness through this program. Most hospitals now have designated officers and offices that are responsible for homeland issues and the training of staff and administration in emergency response.

As for response capacity, hospitals and other medical facilities should have interoperable communications systems, task forces and advisory boards, and a steady stream of communication protocols that interconnect state, local, and federal authorities. Response also implies the capacity to react in the event of an attack. In biological and chemical situations, the medical facility needs adequate stockpiles of vaccine. Medical facilities need to be assured that suitable vendors and companies can supply basic medical goods.

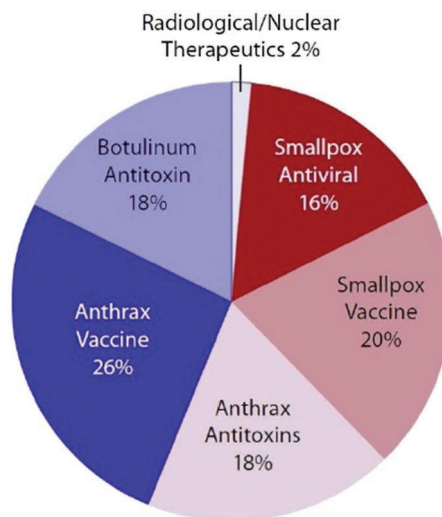
Bioterrorism is primarily a study in science, and the countermeasures need to employ the highest and most sophisticated forms of scientific method. Hospitals should be engaged in serious research that relates to bioterrorism. The study of pathogens and corresponding antidotes should be central to that research, as well as analysis of compounds that will counter the effects of biological agents. Finally, scientific investment should include enhanced laboratory facilities. The Biomedical Advanced Research and Development Authority (BARDA) is one of the chief scientific authorities in R&D. BARDA manages Project BioShield, which includes the procurement and advanced development of medical countermeasures for CBR and nuclear agents, as well as the advanced development and procurement of medical countermeasures for pandemic influenza and other emerging infectious diseases.

11.3.3.1 Project BioShield

The Project BioShield Act³⁰ and the result, Project BioShield, was enacted in 2004.³¹ The general aim of the project was to provide suitable vaccines and other medical supplies in the event of bioterrorism. The overall goals of the program were to

- Expedite the conduct of NIH R&D on medical countermeasures based on the most promising recent scientific discoveries.
- Give the FDA the ability to make promising treatments quickly available in emergency situations.
- Ensure that resources are available to pay for next-generation medical countermeasures (Project BioShield will allow the government to buy improved vaccines or drugs).

Project BioShield's rightful stress is on the pathogens that can cause global damage. Presently, the project has targeted biological threats that either have an antidote or are in need of serious research. Project BioShield reported the funding priorities that directly correlate to the finding of antitoxins and other remedial measures in the event of bioterrorism. BioShield divided up its resources into specific threats and the remedy thereto (Figure 11.16).



Source: Interview at Biomedical Advanced Research and Development Agency, November 2012

Figure 11.16 Project BioShield procurements, for fiscal years 2004–2012. (From Interview at Biomedical Advanced Research and Development Agency, November 2012.)

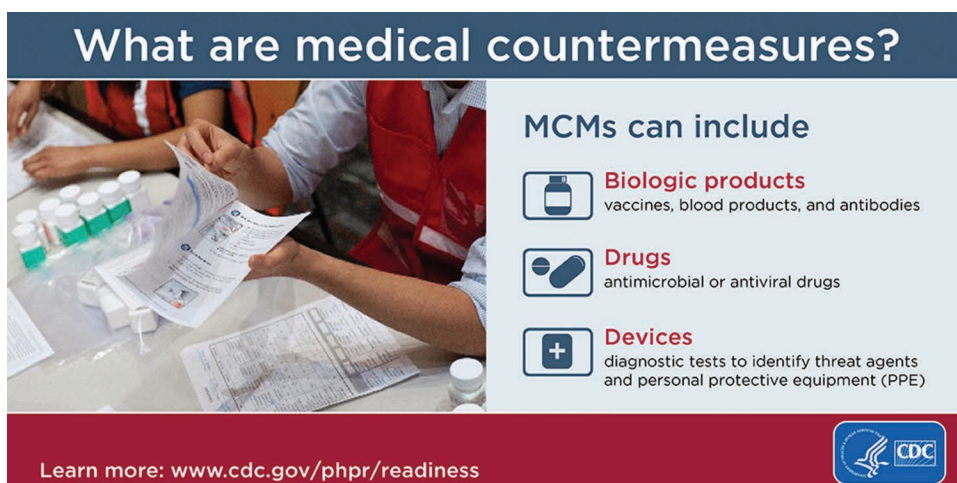


Figure 11.17 The CDC's Website on Medical Countermeasures.

Looked at from another vantage point, BioShield spends the bulk of its research allocation on searching out vaccines for anthrax, smallpox, and botulism. Since 2014, Project BioShield has authored no annual reports even though its funding was extended until 2019. Most of its activities appear to be merged under a new program banner—MedicalCountermeasures.gov. See Figure 11.17.³²

Undoubtedly, the importance of this CDC division has never been as critical as the present as the nation deals with its worst pandemic since 1918.

11.3.3.2 Strategic National Stockpile

The CDC plays a major role in any bioterrorism event. Their most important task in the event of bioterrorism is the maintenance and oversight of the National Pharmaceutical Stockpile (NPS), and the more commonly referred to Strategic National Stockpile (SNS). The stockpile is a repository for lifesaving pharmaceuticals, antibiotics, chemical interventions, as well as medical, surgical, and patient support supplies, and equipment for prompt delivery to the site of a disaster, including a possible biological or chemical terrorist event anywhere in the United States. The SNS serves in a support role to local and state emergency, medical, and public health personnel. And the Stockpile's shortfall as to PPE and other equipment could not have been more obvious in the early days of the pandemic. For a nation as powerful as the United States, to run a shortage on masks is simply unacceptable. The Stockpile is clearly being beefed up as of this writing. See Figure 11.18.³³

A primary purpose of the NPS is to provide critical drugs and medical material that would otherwise be unavailable to local communities. The CDC prioritizes the stockpile based on the seriousness of the threat and the availability of both the agent and the antidote. The stockpile targets biological agents: smallpox, anthrax, pneumonic plague, tularemia, botulinum toxin, and viral hemorrhagic fevers (Figure 11.19).

Internet Exercise: Find out about the many activities of the stockpile at <http://www.cdc.gov/phpr/stockpile/stockpile.htm#sns1>.

11.3.3.3 National Select Agent Registry Program

The CDC net spreads into other territories involving dangerous substances. The National Select Agent Registry Program oversees the use and possession of biological agents and toxins that have the potential to pose a severe threat to public, animal, or plant health. The National Select Agent Registry Program currently requires registration of facilities, including government

U.S. Department of Health & Human Services
Office of the Assistant Secretary for Preparedness and Response

Preparedness Emergency About ASPR

Public Health Emergency
Public Health and Medical Emergency Support for a Nation Prepared

PHE Home > Emergency > Events > 2019 Novel Coronavirus > HHS/ASPR Strategic National Stockpile

Search...

HHS/ASPR Strategic National Stockpile

Response to the COVID-19 Pandemic

The Strategic National Stockpile's role is to supplement state and local supplies during public health emergencies. Many states have products stockpiled, as well. The supplies, medicines, and devices for life-saving care contained in the stockpile can be used as a short-term stopgap buffer when the immediate supply of adequate amounts of these materials may not be immediately available.

As part of the ongoing response, the SNS has deployed personal protective equipment (PPE), including N95 respirators, surgical and face masks, face shields, gloves, and disposable gowns, to help prevent COVID-19 transmission in all 50 states, the nation's four largest cities, and U.S. territories and ventilators to areas in need. The SNS is also working with its partners across the federal government to coordinate logistics operations in order to leverage all available resources to support the COVID-19 response.



Stockpiled Ventilators



Procurement of N95 Respirators



Requesting SNS Assets



Tribal Support



Deploying Medical Supplies



SNS Training Resources

In the Spotlight



COVID-19 Response in Pictures

- B-Roll from the Strategic National Stockpile
- ASPR Newsroom
- Strategic National Stockpile Homepage

COVID-19: Coronavirus Disease 2019

- BARDA's Novel Coronavirus Medical Countermeasure Portfolio
- Working with BARDA on COVID-19 Medical Countermeasures
- Strategic National Stockpile
- Healthcare Provider Resources from ASPR TRACIE
- HPP and Health Care System Preparedness and Response
- Emergency Declarations and Waivers
- Mental and Behavioral Health
- Volunteering and Community Service
- Federal Nutrition Programs for At-Risk Individuals
- Online Training Webinars and Peer-to-Peer Sessions

Figure 11.18 The U.S. Department of Health and Human Services Response to the COVID-19 pandemic.

agencies, universities, research institutions, and commercial entities, that possess, use, or transfer biological agents and toxins that pose a significant threat to the public. Possession, as well as loss or theft of toxins and biological agents, needs to be reported to the CDC. A sample reporting form in the event of loss or theft is provided in Appendix D.



Figure 11.19 CDC stockpiles.

11.4 Pandemic Threats and Public Health

The term *pandemic* connotes many things and generally conjures up images of fear and trepidation. Some pandemics are more serious than others. In the age of COVID-19, we have experienced the severest of virus outbreaks in more than 100 years. A flu outbreak, the nonlethal variety, is a pandemic of sorts. And then there are those outbreaks that are more serious and which cause death on a global scale, such as bird flu—the H1N1 virus where nearly 300 people died worldwide (Figure 11.20). While a large number, that death toll pales in comparison to the COVID-19 toll.

The World Health Organization declared H1N1 the start of the first flu pandemic in 40 years. CDC estimates that between 151,700 and 575,400 people died worldwide from the 2009 H1N1 virus infection during the first year the virus circulated. That H1N1 virus has never been fully cured nor a vaccine discovered. See Figure 11.21.

At other levels of potential destruction, the fears are well founded, for pandemic instances are global in scope and have the capacity to injure and kill on a widespread basis.³⁴ Ebola surely ranks up in the higher echelon of threats on the African continent. While the spread appears in check in 2015–2016, the re-emergence is very likely in the years ahead (Figure 11.22). The Ebola virus ravaged large parts of the African continent and caused dread in that population.

After 2009–2010, another virus, colloquially labelled the “swine flu” emerged. While humans generally do not catch the flu or other virus from pigs, this was apparently taking place—especially in areas with large hog populations. The CDC summarizes how we catch the virus as such:

Most commonly, human infections with variant viruses occur in people with exposure to infected pigs (e.g., children near pigs at a fair or workers in the swine industry). This is thought to happen mainly when an infected pig coughs or sneezes and droplets with influenza virus in them spread through the air. If these droplets land in your nose or mouth, or are inhaled, you can be infected. There also is some evidence that you might get infected by touching something that has virus on it and then touching your own mouth or nose. A third way to possibly get infected is to inhale particles containing influenza virus. Scientists aren’t really sure which of these ways of spread is the most common.³⁵

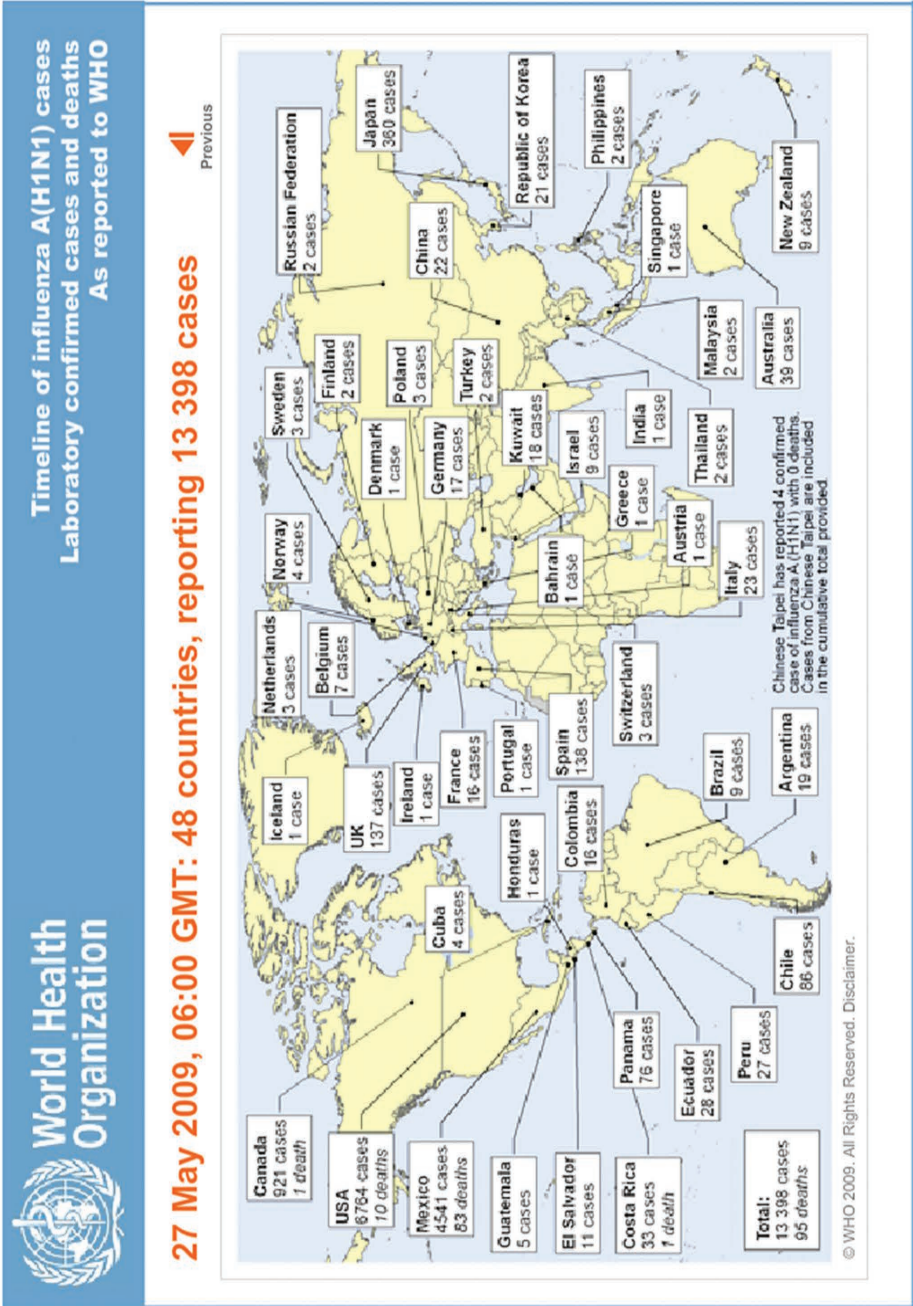


Figure 11.20 Timeline of influenza A (H1N1) cases. (From WHO, Timeline of influenza A(H1N1) cases: Laboratory confirmed cases and deaths as reported to WHO, http://www.who.int/csr/disease/swineflu/history_map/InfluenzaA_H1N1_maps.html.)

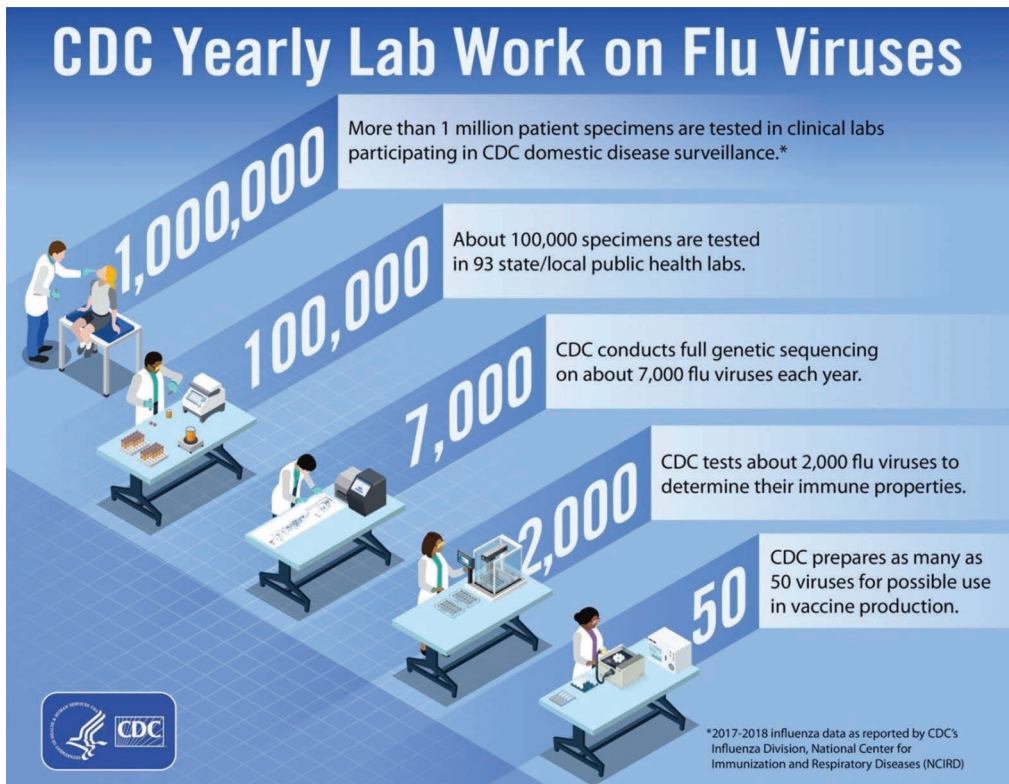


Figure 11.21 Information Sheet on the CDC's lab work on flu viruses.

See Figure 11.23

During the first year of the Swine Flu, labelled H1N1pdm09, some 175,000–575,000 persons died across the world. The disease has continued and not been eradicated nor positively impacted by a vaccine. The CDC indicates that the virus still to this day impacts people and over the next decade would cause enormous damage. See Figure 11.24.³⁶

Pandemics are not a new phenomenon but have long been tracked globally. Pandemics fall into these basic categories:

- Bird flu is commonly used to refer to AI (see the following category). Bird flu viruses infect birds, including chickens, other poultry, and wild birds such as ducks.
- AI is caused by influenza viruses that occur naturally among wild birds. Low-pathogenic AI is common in birds and causes few problems. Highly pathogenic H5N1 is deadly to domestic fowl, can be transmitted from birds to humans, and is deadly to humans. There is virtually no human immunity and human vaccine availability is very limited.
- Pandemic flu is virulent human flu that causes a global outbreak, or pandemic, of serious illness. Because there is little natural immunity, the disease can spread easily from person to person. Currently, the world is experiencing the Covid-19 virus in ways rarely seen since the 1918 Spanish Flu. Today, there is a bona fide, world-wide pandemic, impacting the entire world, though there are a number of promising vaccines in development and on the horizon.
- Seasonal (or common) flu is a respiratory illness that can be transmitted person to person. Most people have some immunity, and a vaccine available.³⁷

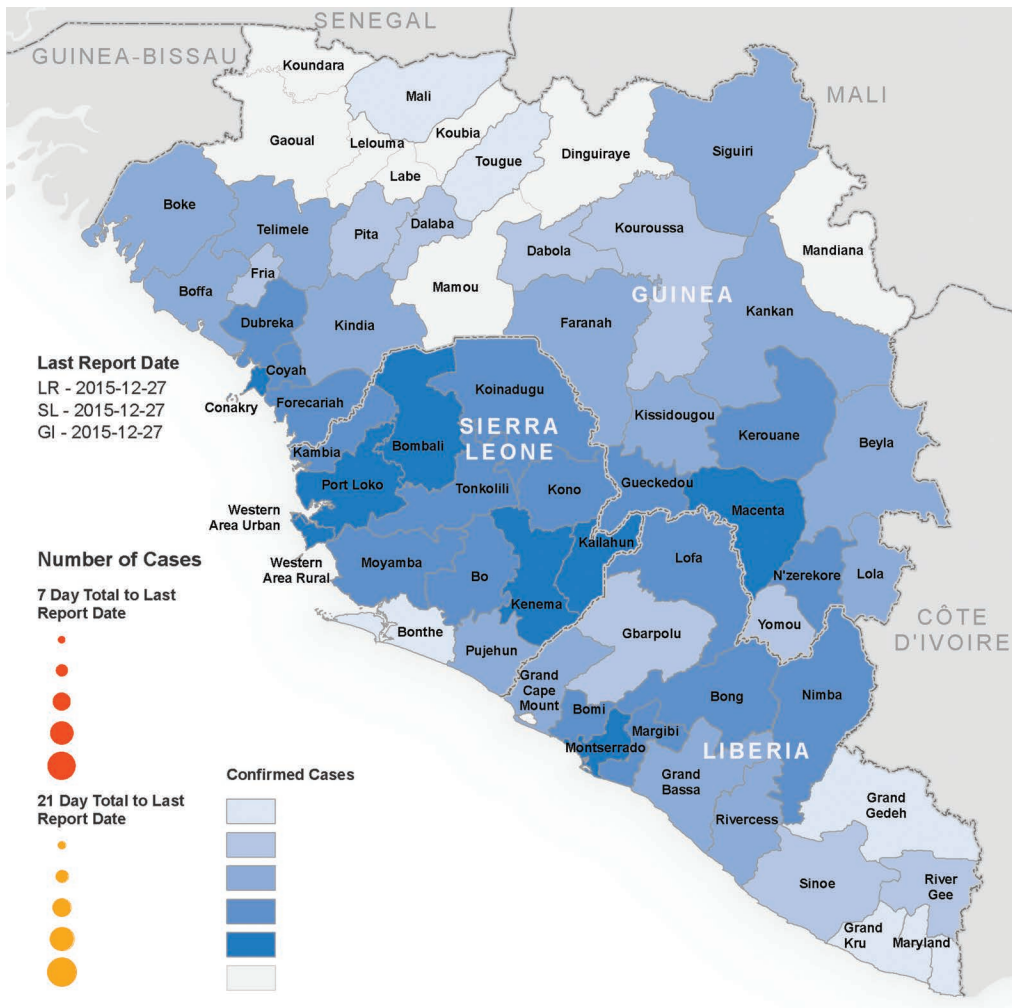


Figure 11.22 Geographical distribution of new and total confirmed Ebola cases in Guinea, Liberia, and Sierra Leone, January 6, 2016. (From WHO, *Ebola Situation Report*, January 6, 2016 (accessed February 7, 2016).)

To compare and contrast the pandemic form with other sorts of flu or influenza, see Figure 11.25.

Pandemics are largely the by-product of influenzas (Figure 11.26). Influenza viruses have mutated and caused pandemics or global epidemics. In the United States, the most severe outbreaks occurred in 1918 (Figures 11.27 and 11.28).

Internet Exercise: For a history of flu epidemics, visit <https://www.cdc.gov/flu/pandemic-resources/1918-commemoration/1918-pandemic-history.htm>.

The very definition of pandemic implies a broad impact, a disease or infection with the capacity to cover a large swath of geography. A pandemic is a global disease outbreak. For example, a flu pandemic occurs when a new influenza virus emerges for which people have little or no immunity, and for which there is no vaccine. Or a disease may be spread in an airborne fashion, such as the avian influenza witnessed in China and other Asian locales. The World Health Organization (WHO) gauges the severity of influenza outbreak by phases—with the infection commencing in lower animal forms, progressing to various levels of human infection,

FLU CAN SPREAD BETWEEN PIGS AND PEOPLE

Information for people exposed to pigs, including people who enter the swine barns at agricultural fairs or people who raise pigs for show or farming

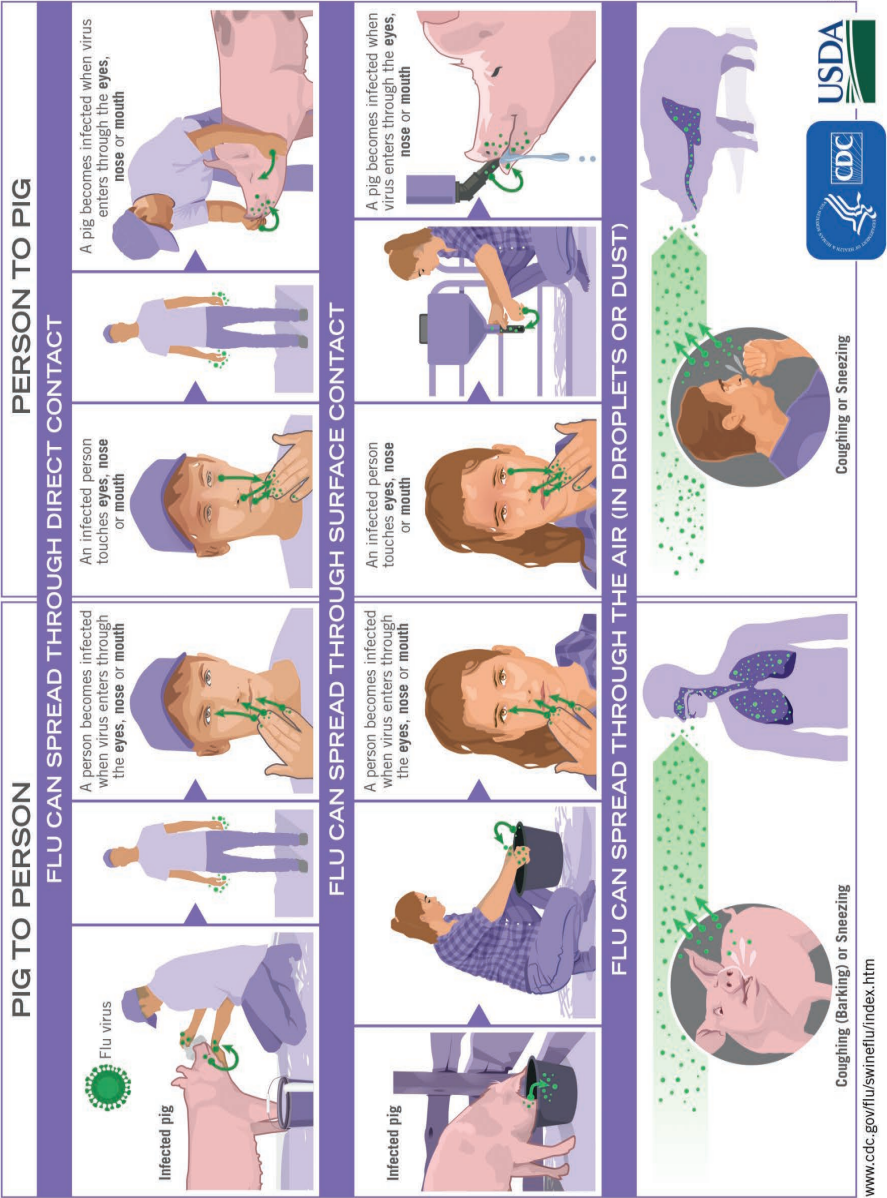


Figure 11.23 Illustration of swine flu transmission between pigs and humans. (CDC and USDA, at <https://www.cdc.gov/flu/pdf/swineflu/transmission-between-pigs-people.pdf>.)

The burden of influenza A H1N1pdm09 virus from 2009 to 2018

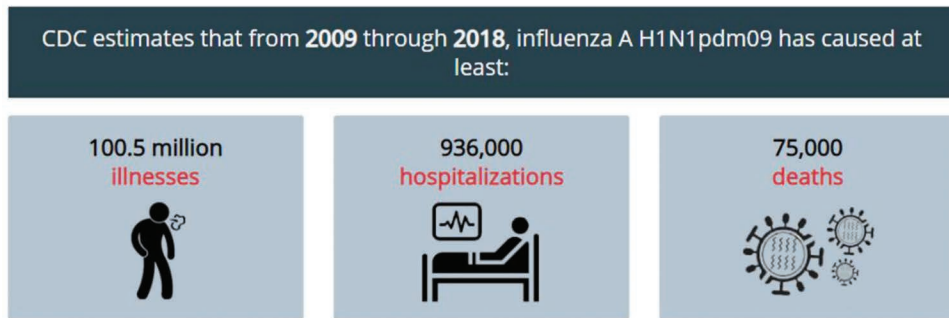


Figure 11.24 The continued persistence of H1N1pdm09.

to eventual reductions.³⁸ It is difficult to predict when the next influenza pandemic will occur or how severe it will be as is obvious and self-evident in the COVID-19 event. Clearly, no one saw, predicted or anticipated the staggering consequences of our present pandemic. Who would have ever envisioned a New York City empty and barren of people—most of whom hunkered down in shuttered environments? See Figure 11.29.

Wherever and whenever a pandemic starts, everyone around the world is at risk. Countries might, through measures such as border closures and travel restrictions, delay the arrival of the virus, but they cannot stop it. Health professionals are concerned that the continued spread of a highly pathogenic avian H5N1 virus across Eastern Asia and other areas represents a significant threat to human health. The H5N1 virus has raised concerns about a potential human pandemic because

- It is especially virulent.
- It is being spread by migratory birds.
- It can be transmitted from birds to mammals and, in some limited circumstances, to humans.
- Like other influenza viruses, it continues to evolve.

Pandemics have been witnessed throughout human history, with the twentieth century experiencing myriad events. The National Institute of Health tracks the past 100 years (Figure 11.30). Though COVID has been with us a relatively short time, its severity and brutality have altered so many aspects of human operations that it feels like a lifetime.

11.4.1 COVID-19: The Pandemic from China

During the summer of 2019, there were murmurings of a new virus in the Wuhan region of China. Even at its earliest stages, the virus was a formidable challenge to health authorities. By the Fall of 2019, the virus, concentrated in the City of Wuhan, China, began to multiply at an alarming rate. Health officials were startled by the pace of its spread and the virulent reactions of its victims. In addition, the virus tended to create diverse sets of pathology—with some patients suffering respiratory ailments, while others suffered from neurological issues. The range of impacts varied by patient and also by region. In the early days of the pandemic in China, the Chinese government was less than forthright about its severity and the implications for spread. In fact, the Chinese government, knowing full well of its dangers, did little to restrict travel or warn the rest of the civilized world about the disease.³⁹ What is clear is the Chinese government,

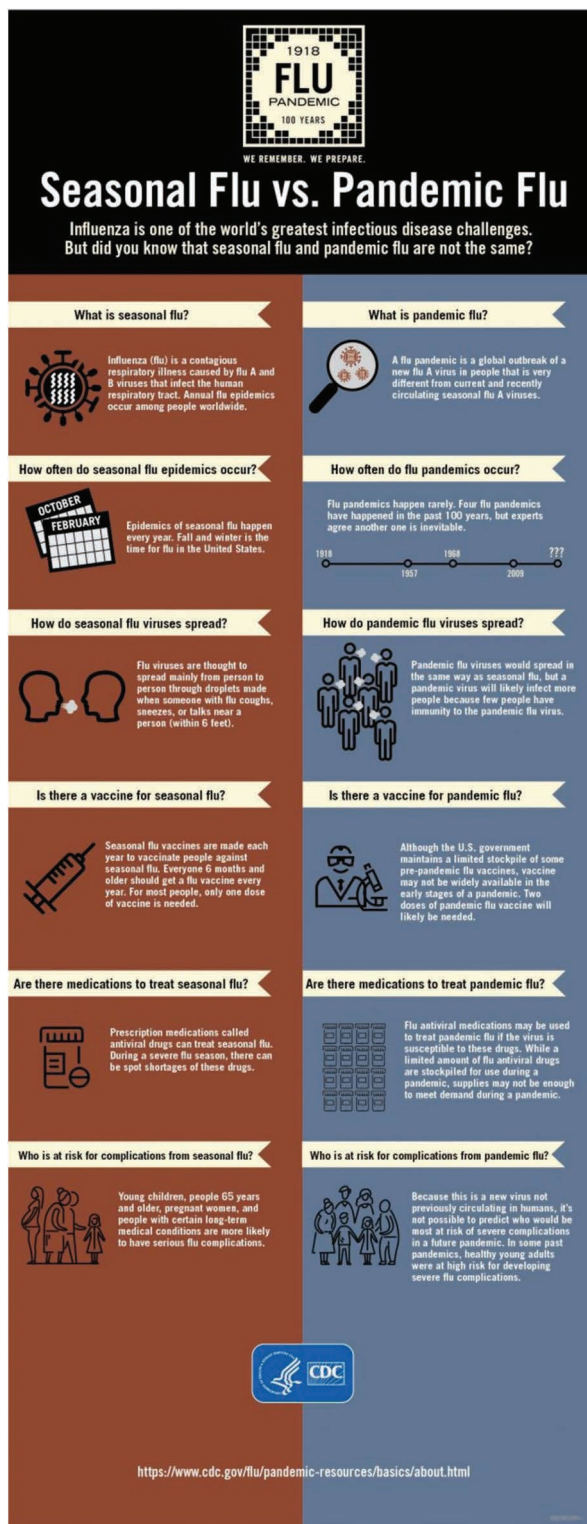


Figure 11.25 Seasonal flu vs. pandemic flu.

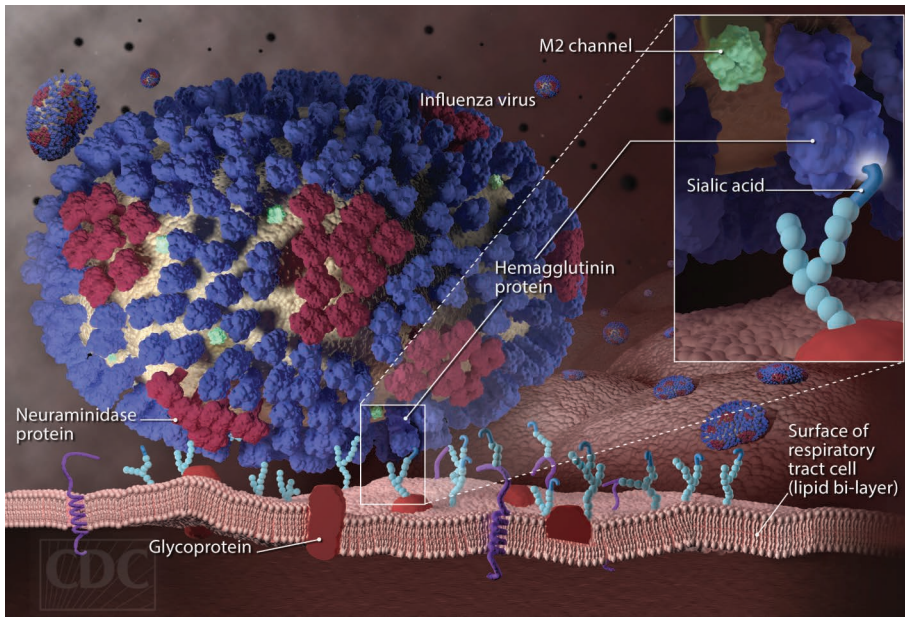


Figure 11.26 This image illustrates the very beginning stages of an influenza (flu) infection. Most experts think that influenza viruses spread mainly through small droplets containing influenza virus. These droplets are expelled into the air when people infected with the flu cough, sneeze, or talk. Once in the air, these small infectious droplets can land in the mouths or noses of people who are nearby. (From CDC, Influenza (flu), <http://www.cdc.gov/flu/images.htm> (accessed February 7, 2016).)



Figure 11.27 In July, an American soldier said that while influenza caused a heavy fever, it “usually only confines the patient to bed for a few days.” The mutation of the virus changed all that (Credit: National Library of Medicine). (From HHS, The great pandemic: The United States in 1918–1919, http://www.flu.gov/pandemic/history/1918/the_pandemic/influenza/index.html.)

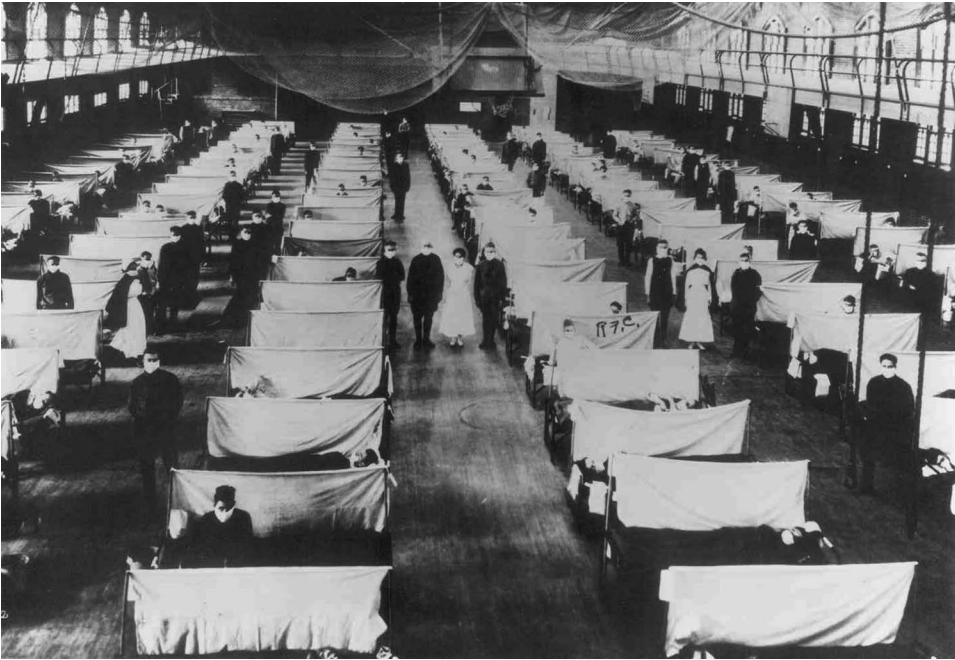


Figure 11.28 When it came to treating influenza patients, doctors, nurses, and druggists were at a loss (Credit: Office of the Public Health Service Historian). (From HHS, The great pandemic, http://www.flu.gov/pandemic/history/1918/the_pandemic/iowa_flu2.jpg.)



Figure 11.29 March 2020: Empty streets of New York at Times Square 42nd street during pandemic virus Covid-19. (Courtesy Shutterstock.com.)

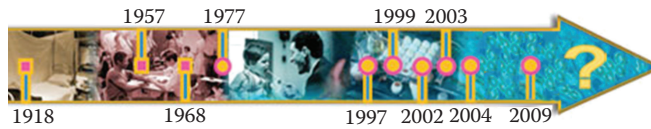


Figure 11.30 Timeline of human flu pandemics, including human cases of avian and swine influenza viruses. (From National Institute of Allergy and Infectious Diseases, National Institute of Health, Timeline of human flu pandemics, <http://www.niaid.nih.gov/topics/flu/research/pandemic/pages/timelinehumanpandemics.aspx>.)

throughout the Fall of 2019, did not make readily available its data and findings on the disease; did not restrict the movement of its affected populations and downplayed the significance and severity to the World Health Organization and other international organizations.⁴⁰

Only when the outbreak in Wuhan City, China could no longer be contained or controlled, did it spill out into the world's recognition. For in Wuhan, Chinese authorities, throughout the late Fall of 2019 and into early January, took draconian steps to control the spread. Wuhan became a city in complete lockdown, but not before it had migrated and taken root in other countries around the world. See Figure 11.31.

Wuhan citizens carrying the disease travelled without much restriction early on—to Europe and the United States. President Trump shut down travel to the United States and China on January 31, 2020. While there were nearly no cases in the United States the spread was already underway in Seattle, New York City, Boston, and Los Angeles. Despite this, New York City became the epicenter for the disease in the United States. The Confirmed Death Rate for COVID-19 for the five boroughs of New York City paints a picture without rival in the United States. See Figure 11.32.⁴¹

Hospitalizations, infection rates, and most importantly the power and capacity of New York City to spread the virus throughout surrounding states and the entire country have been largely demonstrated. While stay at home orders were posted, travel restrictions within the United States were not and the spread from such a massive infected population was inevitable.



Figure 11.31 Testing in Wuhan, China. (Source: Voice of America.)

Daily Reported Death Totals

New York City's first confirmed COVID-19 death was reported on March 11.

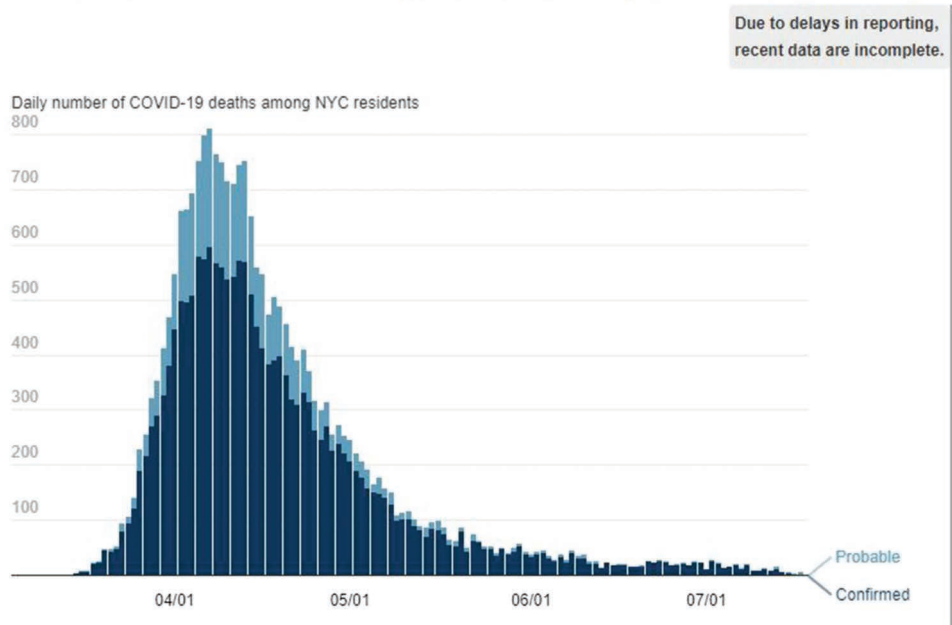


Figure 11.32 Daily reported death tolls in New York City.

The *New York Times* refers to this reality as “seeding” the rest of the country.⁴² See Figure 11.33.⁴³ From its very outset, the virus appeared a more ravishing version than its predecessors. Its very shape, with crowns throughout, as if barbed edges, had the unusual capacity of attaching to lungs and destroying respiratory capacity. See Figure 11.34.

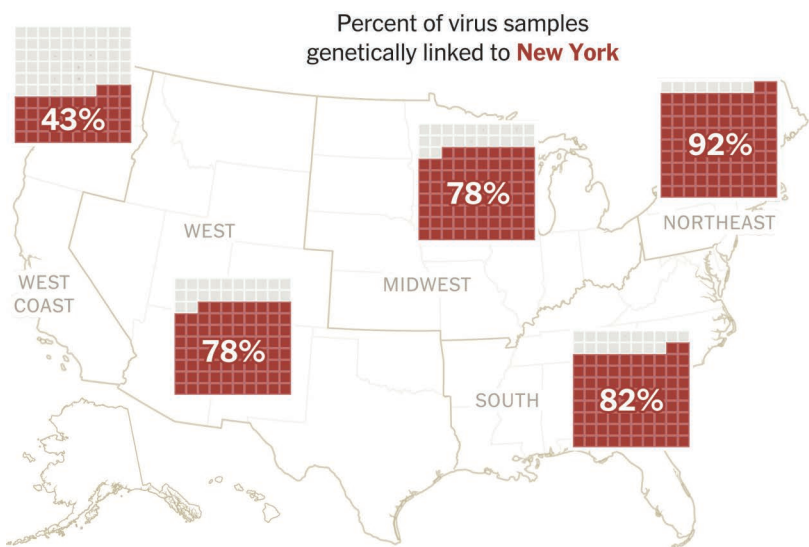


Figure 11.33 Percentage of virus samples linked to New York.

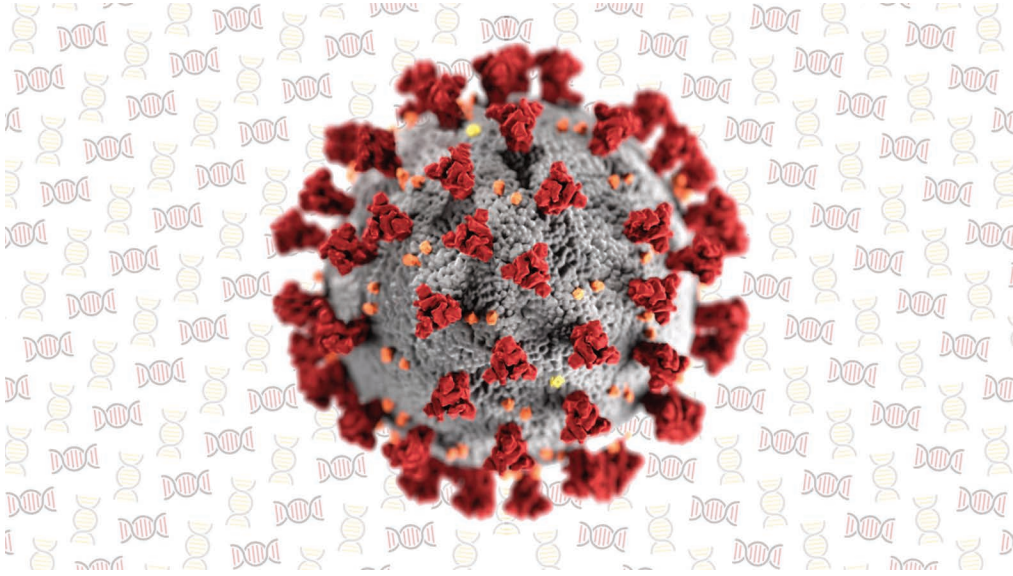


Figure 11.34 The COVID-19 virus.

Each organ of the body seems more than usually traumatized than other viruses. Lungs have even been permanently damaged. See Figure 11.35.

By the end of March, the impact of the virus was starting to be felt across the general population and a steady climb was in store for the next few months. What once appeared to be potentially checked and controlled, despite lockdowns and a host of precautionary measure, was now on an aggressive upward trajectory. By late July of 2020, any hopes of a “flattening out” of the growth curve had been largely forgotten. See Figure 11.36.⁴⁴

Internet Exercise: Use the DHS Datatracker to discover the full implications of the disease in the United States at <https://www.cdc.gov/covid-data-tracker/index.html#cases>.

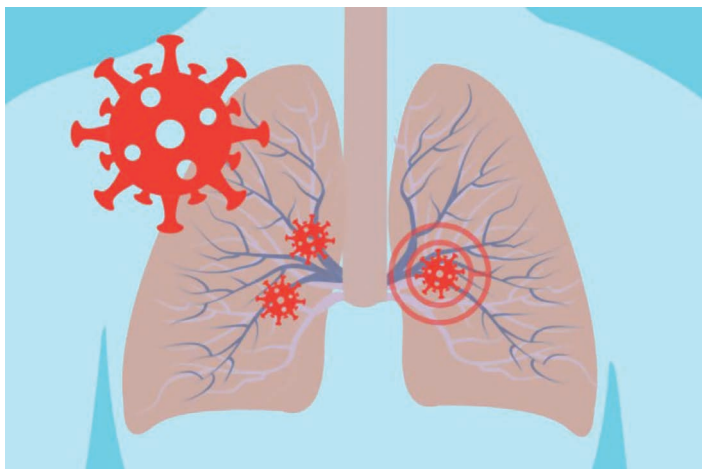


Figure 11.35 While numerous organs have been show to be effected by COVID-19, the lungs are consistently the most impacted by the virus. (Source: Cleveland Clinic.)

Homeland Security

New Cases by Day

The following chart shows the number of new COVID-19 cases reported each day in the U.S. since the beginning of the outbreak. Hover over the bars to see the number of new cases by day.

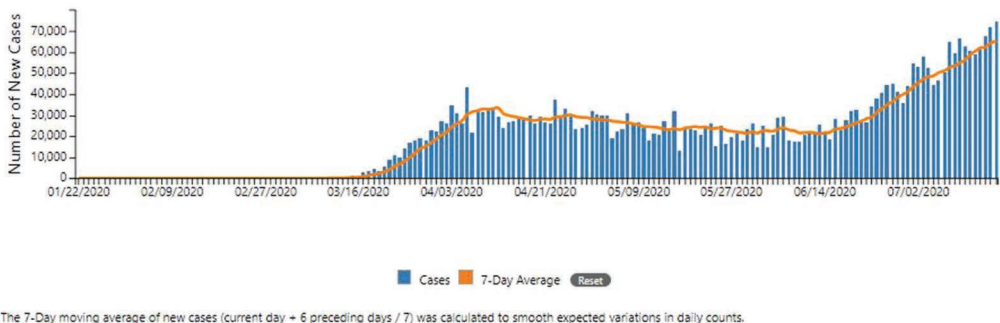


Figure 11.36 New cases by day through July 2020.

Throughout the spring of 2020 and moving into the summer, and after months of lockdowns and social distancing, the pace of the infections and rates of death started to show promise. State governments long advocated for these policies and when improved, would allow a re-opening of sorts. Some did in phases; others measured in a color-coded system of red, yellow and green. Opening up would have to be gradual and sensitive to safety by continued social distancing and the wearing of masks.

Some states, like Texas and Florida, would more aggressively reopen but results afterward showed a dramatic rise in cases. The balance of reopening postures, a nation in need of economic growth, and the citizen's hopes to return to work, is not an easy task. Sitting at home the rest of one's life is healthy for neither children nor adults, but moving back into a full lifestyle without proper caution is unwise as well. The culture will have to experiment a bit on the return to normalcy and it may be that certain activities will have slower return than others. It is a fair restriction to halt large-scale events, conferences, exhibit halls, sporting and entertainment, political rallies, and the like because these become new "seeders." Schools, colleges, and universities could be the most challenging environment. While all agree that it is unhealthy for our youth to be trapped in a virtual world for school, the growing discovery of the young now suffering from COVID-19 raises additional concerns about reopening. Schools are laboratories for the disease as are dormitories and dining halls. Just recently both France and Israel, who had just reopened their schools, suffered a wave of COVID-19 cases and had to shut them down again.⁴⁵ What is certain is the variability and changeability of these conditions under the COVID-19 reality. As of July 2021, the Biden administration's vaccination rollout program has led to large-scale vaccinations and a lifting of numerous restrictions in many parts of the country. Despite this, the new Delta strain is leading to another surge due to unvaccinated individuals: both those too young to be eligible for vaccination or those hesitant to get vaccinated.

11.4.2 Planning, Preparedness, and Response to the Pandemic

Recognizing both the epidemiological and terrorist implications of the pandemic, state, federal, and local governments need to prepare for and respond to this event.⁴⁶ Globally, the WHO has a system of alerts and notices as to potential or actual pandemics, although under present leadership, the agency had come under criticism for now providing

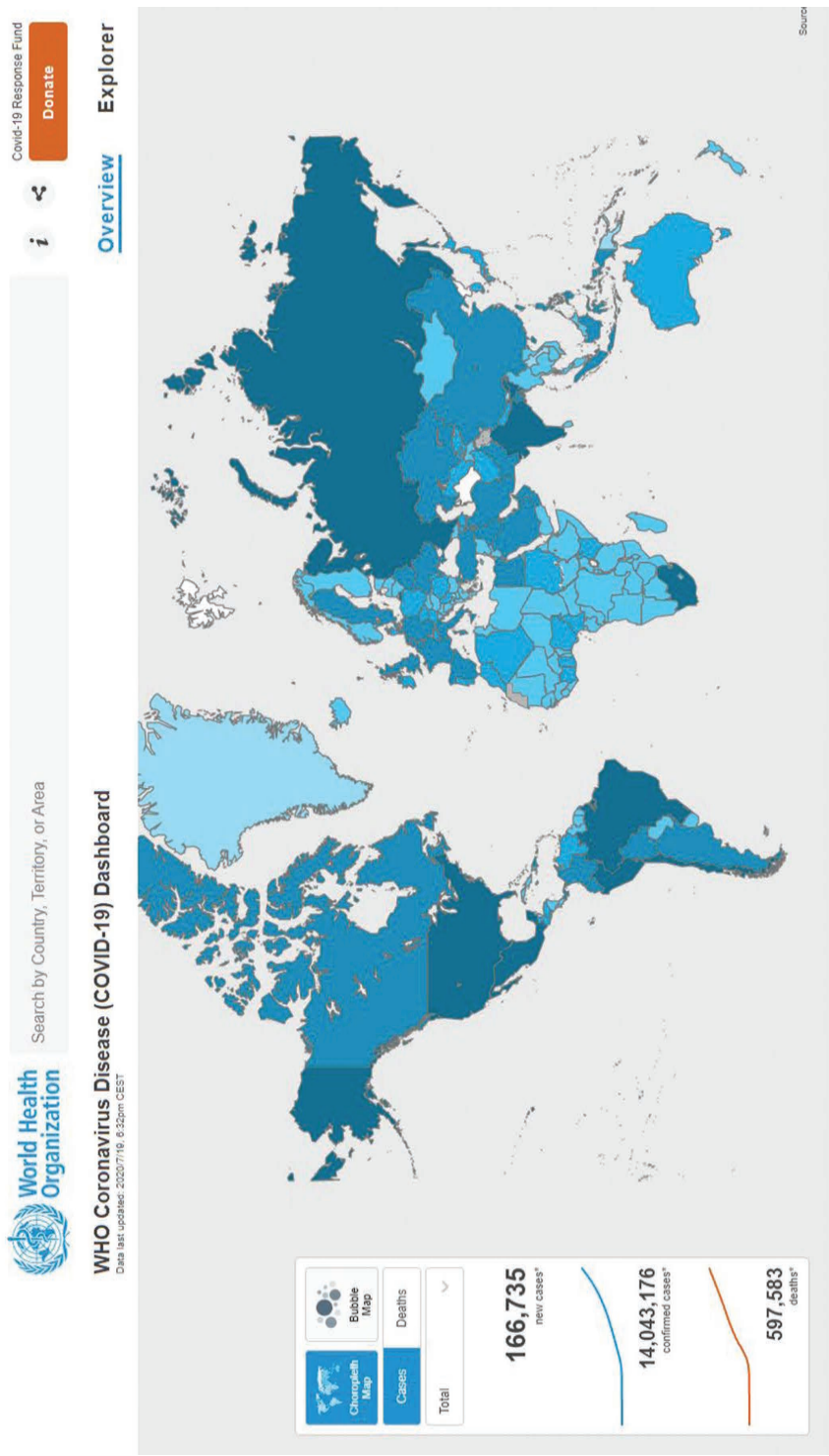
accurate warnings or advice on the severity of the outbreak. For example, WHO was late designating COVID-19 as a pandemic and appeared early on to downplay its worldwide implications. Each day, the WHO publishes existing or developing threats, an example being Figure 11.37.⁴⁷

At the federal level, a prevention and response program has been formalized and by most governmental agencies. While the DHS, HHS, and the CDC have taken the lead, most government agencies have issued advice on the virus. The National Strategy for Pandemic Influenza guides the country's preparedness and response to an influenza pandemic, with the intent of (1) stopping, slowing, or otherwise limiting the spread of a pandemic to the United States; (2) limiting the domestic spread of a pandemic, and mitigating disease, suffering, and death; and (3) sustaining infrastructure and mitigating impact to the economy and the functioning of society.⁴⁸

The strategy charges HHS with leading the federal pandemic preparedness. Working with the WHO, federal officials seek to mitigate and contain as well as prevent future events from taking place (Figure 11.38).

The key elements in planning and response for pandemics include the following:

1. In advance of an influenza pandemic, HHS will work with federal, state, and local government partners and the private sector to coordinate pandemic influenza preparedness activities and to achieve interoperable response capabilities.
2. In advance of an influenza pandemic, HHS will encourage all Americans to be active partners in preparing their states, local communities, workplaces, and homes for pandemic influenza and will emphasize that a pandemic will require Americans to make difficult choices. An informed and responsive public is essential to minimizing the health effects of a pandemic and the resulting consequences to society.
3. In advance of an influenza pandemic, HHS, in concert with federal partners, will work with the pharmaceutical industry to develop domestic vaccine production capacity sufficient to provide vaccines for the entire U.S. population as soon as possible after the onset of a pandemic and, during the pre-pandemic period, to produce up to 20 million courses of vaccine against each circulating influenza virus with pandemic potential and to expand seasonal influenza domestic vaccine production to cover all Americans for whom vaccine is recommended through normal commercial transactions.
4. In advance of an influenza pandemic, HHS, in concert with federal partners and in collaboration with the states, will procure sufficient quantities of antiviral drugs to treat 25% of the U.S. population and, in so doing, stimulate development of expanded domestic production capacity sufficient to accommodate subsequent needs through normal commercial transactions. HHS will stockpile antiviral medications in the Strategic National Stockpile, and states will create and maintain local stockpiles.
5. Sustained human-to-human transmission anywhere in the world will be the triggering event to initiate a pandemic response by the United States. Because we live in a global community, a human outbreak anywhere means risk everywhere.
6. The United States will attempt to prevent an influenza pandemic or delay its emergence by striving to arrest isolated outbreaks of a novel influenza wherever circumstances suggest that such an attempt might be successful, acting in concert with WHO and other nations as appropriate. At the core of this strategy will be basic public health measures to reduce person-to-person transmission.



Globally, as of 6:32pm CEST, 19 July 2020, there have been 14,043,176 confirmed cases of COVID-19, including 597,583 deaths, reported to WHO.

Figure 11.37 WHO COVID-19 Dashboard.

11.4 Pandemic Threats and Public Health

Phase 1	No animal influenza virus circulating among animals has been reported to cause infection in humans.
Phase 2	An animal influenza virus circulating in domesticated or wild animals is known to have caused infection in humans and is therefore considered a specific potential pandemic threat.
Phase 3	An animal or human-animal influenza reassortant virus has caused sporadic cases or small clusters of disease in people, but has not resulted in human-to-human transmission sufficient to sustain community-level outbreaks.
Phase 4	Human-to-human transmission (H2H) of an animal or human-animal influenza reassortant virus able to sustain community-level outbreaks has been verified.
Phase 5	The same identified virus has caused sustained community level outbreaks in two or more countries in one WHO region.
Phase 6	In addition to the criteria defined in Phase 5, the same virus has caused sustained community level outbreaks in at least one other country in another WHO region.
Post-peak period	Levels of pandemic influenza in most countries with adequate surveillance have dropped below peak levels.
Possible new wave	Level of pandemic influenza activity in most countries with adequate surveillance rising again.
Post-pandemic period	Levels of influenza activity have returned to the levels seen for seasonal influenza in most countries with adequate surveillance.

Figure 11.38 Global pandemic phases and the stages for federal government response. (From FEMA, *Pandemic Influenza Continuity of Operations Annex Template Instructions*, 13, <http://www.fema.gov/media-library-data/1396880633531-35405f61d483668155492a7cccd1600b/Pandemic+Influenza+Template.pdf>.)

7. At the onset of an influenza pandemic, HHS, in concert with federal partners, will work with the pharmaceutical industry to procure vaccine directed against the pandemic strain and to distribute vaccine to state and local public health departments for predetermined priority groups based on preapproved state plans.
8. At the onset of an influenza pandemic, HHS, in collaboration with the states, will begin to distribute and deliver antiviral drugs from public stockpiles to healthcare facilities and others with direct patient care responsibility for administration to predetermined priority groups.⁴⁹

Internet Exercise: Review the essential planning elements for a pandemic influenza outbreak as recommended by FEMA at https://www.fema.gov/pdf/about/org/ncp/pandemic_influenza.pdf.

Pandemic planning also incorporates the resources of state and local law enforcement—agencies that are on the front lines throughout this public health threat (Figure 11.39).⁵⁰

Every entity of government and the private sector should anticipate and prepare for the potential pandemic. As in all other areas of homeland security planning, the agency must be predictive yet reasonable in its approach and anticipate the required resource in the event of a pandemic.

Internet Exercise: See data from the CDC on how influenza is tracked at www.cdc.gov/flu/weekly/index.htm.

LAW ENFORCEMENT PANDEMIC INFLUENZA PLANNING CHECKLIST



In the event of pandemic influenza, law enforcement agencies (e.g., State, local, and tribal Police Departments, Sheriff's Offices, Federal law enforcement officers, special jurisdiction police personnel) will play a critical role in maintaining the rule of law as well as protecting the health and safety of citizens in their respective jurisdictions. Planning for pandemic influenza is critical.

To assist you in your efforts, the Department of Health and Human Services (HHS) has developed the following checklist for law enforcement agencies. This checklist provides a general framework for developing a pandemic influenza plan. Each agency or organization will need to adapt this checklist according to its unique needs and circumstances. The key planning activities in this checklist are meant to complement and enhance your existing all-hazards emergency and operational continuity plans. Many of the activities identified in this checklist will also help you to prepare for other kinds of public health emergencies.

Information specific to public safety organizations and pandemic flu preparedness and response can be found at <http://www.ojp.usdoj.gov/BJA/pandemic/resources.html>. For further information on general emergency planning and continuity of operations, see www.ready.gov. Further information on pandemic influenza can be found at www.pandemicflu.gov.

Develop a pandemic influenza preparedness and response plan for your agency or organization.

Completed	In Progress	Not Started	
☐	☐	☐	Assign primary responsibility for coordinating law enforcement pandemic influenza preparedness planning to a single person (identify back-ups for that person as well) with appropriate training and authority (insert name, title, and contact information here).
☐	☐	☐	Form a multidisciplinary law enforcement/security planning committee to address pandemic influenza preparedness specifically. The planning team should include at a minimum: human resources, health and wellness, computer support personnel, legal system representatives, partner organizations, and local public health resources. Alternatively, pandemic influenza preparedness can be addressed by an existing committee with appropriate skills and knowledge and relevant mission (list committee members and contact information here). This Committee needs to have the plan approved by the Agency Head.
☐	☐	☐	Review Federal, State, and local public health and emergency management agencies' pandemic plans in areas where you operate or have jurisdictional responsibilities. Ensure that your plan is NIMS (National Incident Management System) compliant and align your plan with the local Incident Command System (ICS) and local pandemic influenza plans to achieve a unified approach to incident management. See "State and Local Governments," www.pandemicflu.gov/plan/states/index.html and http://www.fema.gov/emergency/nims/index.shtml .
☐	☐	☐	Verify Command and Control areas of responsibility and authority during a pandemic. Identify alternative individuals in case primary official becomes incapacitated.
☐	☐	☐	Set up chain of command and procedures to signal activation of the agency's response plan, altering operations (e.g., shutting down non-critical operations or operations in affected areas or concentrating resources on critical activities), as well as returning to normal operations.
☐	☐	☐	Determine the potential impact of a pandemic on the agency or organization by using multiple possible scenarios of varying severity relative to illness, absenteeism, supplies, availability of resources, access to legal system representatives, etc. Incorporate pandemic influenza into agency emergency management planning and exercise.
☐	☐	☐	Identify current activities (by location and function) that will be critical to maintain during a pandemic. These essential functions might include 911 systems in communities where law enforcement is responsible for this activity, other communications infrastructures, community policing, information systems, vehicle maintenance, etc. Identify critical resources and inputs (e.g., employees, supplies, subcontractor services/products, and logistics) that are necessary to support these crucial activities.

September 4, 2007
Version 1



Figure 11.39 Law enforcement pandemic influenza planning checklist from the CDC. (From HHS, Law enforcement pandemic influenza planning checklist, www.flu.gov/planning-preparedness/business/lawenforcement.pdf.)

(Continued)

11.4 Pandemic Threats and Public Health

Develop a pandemic influenza preparedness and response plan for your agency or organization *(continued)*

Completed	In Progress	Not Started	
☐	☐	☐	Develop, review, and approve an official law enforcement/security pandemic influenza preparedness and response plan. This plan represents the output of many or all of the activities contained in this checklist. This plan can be an extension of your current emergency or business continuity plans with a special focus on pandemic influenza and should identify the organizational structure to be used to implement the plan. Include procedures to implement the plan in stages based upon appropriate triggering events.
☐	☐	☐	Develop a pandemic-specific emergency communications plan as part of the pandemic influenza preparedness and response plan, and revise it periodically. The communications plan should identify a communication point of contact, key contacts and back-ups, and chain of communications and clearance. Plan may also include potential collaboration with media representatives on the development of scripts based on likely scenarios guided by the public information officer(s). Coordinate with partners in emergency government and public health in advance.
☐	☐	☐	Designate an individual to monitor pandemic status and collect, organize, and integrate related information to update operations as necessary. Develop a plan for back-up if that person becomes ill during a pandemic. Develop a situational awareness capability that leadership can use to monitor the pandemic situation, support agency decisions, and facilitate monitoring of impact.
☐	☐	☐	Distribute pandemic plan throughout the agency or organization and develop means to document employees/staff received and read the plan.
☐	☐	☐	Allocate resources through the budgeting process as needed to support critical components of preparedness and response identified in your plan.
☐	☐	☐	Periodically test both the preparedness and response plan and the communications plan through drills and exercises; incorporate lessons learned into the plans.

Plan for the impact of a pandemic on your employees

Completed	In Progress	Not Started	
☐	☐	☐	Develop contingency plans for 30 – 40% employee absences. Keep in mind that absences may occur due to personal illness, family member illness, community mitigation measures, quarantines, school, childcare, or business closures, public transportation disruptions, or fear of exposure to ill individuals, as well as first responder, National Guard, or military reserve obligations.
☐	☐	☐	As necessary, plan for cross-training employees, use of auxiliary personnel and recent retirees, recruiting temporary personnel during a crisis, or establishing flexible worksite options (e.g., telecommuting) and flexible work hours (e.g. staggered shifts) when appropriate.
☐	☐	☐	Develop a reporting mechanism for employees to immediately report their own possible influenza illness during a pandemic (24/7).
☐	☐	☐	Establish compensation and leave policies that strongly encourage ill workers to stay home until they are no longer contagious. During a pandemic, employees with influenza-like symptoms (such as fever accompanied by sore throat, muscle aches and cough) should not enter the worksite to keep from infecting other workers. Employees who have been exposed to someone with influenza, particularly ill members of their household, may also be asked to stay home and monitor their symptoms.
☐	☐	☐	Employees who develop influenza-like symptoms while at the worksite should leave as soon as possible. Consult with State and local public health authorities regarding appropriate treatment for ill employees. Prepare policies that will address needed actions when an ill employee refuses to stay away from work. Federal agencies can consult guidance provided by the Office of Personnel Management (OPM) at www.opm.gov/pandemic .
☐	☐	☐	Identify employees who may need to stay home if schools dismiss students and childcare programs close for a prolonged period of time (up to 12 weeks) during a severe pandemic. Advise employees not to bring their children to the workplace if childcare cannot be arranged. Plan for alternative staffing or staffing schedules on the basis of your identification of employees who may need to stay home.
☐	☐	☐	Identify critical job functions and plan now for cross-training employees to cover those functions in case of prolonged absenteeism during a pandemic. Develop succession plans for each critical agency position to ensure the continued effective performance of your organization by identifying and training replacements for key people when necessary. These replacements should be integrated into employee development activities, and should include critical contracted services as well.
☐	☐	☐	Develop policies that focus on preventing the spread of respiratory infections in the workplace. This policy might include social distancing practices, the promotion of respiratory hygiene/cough etiquette, the creation of screening mechanisms for use during a pandemic to examine employees for fever or influenza symptoms, using the full range of available leave policies to facilitate staying home when ill or when a household member is ill, and appropriate attention to environmental hygiene and cleaning. (For more information see the www.pandemicflu.gov and http://www.pandemicflu.gov/plan/community/mitigation.html as well as OPM's guidance at www.opm.gov/pandemic .)

2

Figure 11.39 (CONTINUED) Law enforcement pandemic influenza planning checklist from the CDC. (From HHS, Law enforcement pandemic influenza planning checklist, www.flu.gov/planning-preparedness/business/lawenforcement.pdf.)

(Continued)

Homeland Security

Plan for the impact of a pandemic on your employees *(continued)*

Completed	In Progress	Not Started	
☐	☐	☐	Provide educational programs and materials (language, culture, and reading-level appropriate) to personnel on: • pandemic fundamentals (e.g., signs and symptoms of influenza, modes of transmission, medical care), • personal and family protection and response strategies (e.g., hand hygiene, coughing/sneezing etiquette, etc.). Post instructional signs that illustrate correct infection control procedures in all appropriate locations, including offices, restrooms, waiting rooms, processing rooms, detention facilities, vehicles, etc. and, • community mitigation interventions (e.g., social distancing, etc.). See www.pandemicflu.gov, www.cdc.gov/flu/protect/stopgerms.htm, http://www.cdc.gov/flu/protect/covercough.htm, www.cdc.gov/flu/professionals/infectioncontrol/resphygiene.htm, and http://www.pandemicflu.gov/plan/community/mitigation.html.
☐	☐	☐	Provide training for law enforcement officers, office managers, medical or nursing personnel, and others as needed for performance of assigned emergency response roles. Identify a training coordinator and maintain training records. Ensure all staff are familiar with the local Incident Command System (ICS) and understand the roles and persons assigned within that structure. See http://www.fema.gov/emergency/nims/index.shtm for more information
☐	☐	☐	Stock recommended personal protective equipment (PPE) and environmental infection control supplies and make plans to distribute to employees, contractors, and others (including detainees) as needed. These supplies should include tissues, waste receptacles, single-use disinfection wipes, and alcohol-based hand cleaner (containing at least 60% alcohol). EPA registered disinfectants labeled for human influenza A virus may be used for cleaning offices, waiting rooms, bathrooms, examination rooms, and detention facilities. PPE may include gloves, surgical masks and respirators (disposable N95s or higher respirators or reusable respirators), eye protection, pocket masks (for respiratory resuscitation) and protective cover wear (e.g., impervious aprons). The specific uses for the above supplies will be advised by State and local health officials during a pandemic. Further information can be found at www.pandemicflu.gov and at http://www.osha.gov/Publications/OSHA3327pandemic.pdf.
☐	☐	☐	Provide information to employees to help them and their families prepare and plan for a pandemic. See www.pandemicflu.gov/plan/individual/index.html.
☐	☐	☐	Work with State and/or local public health to develop a plan for distribution of pandemic influenza vaccine and antiviral medications to law enforcement personnel. See current HHS recommendations for pandemic influenza vaccine and antiviral use at http://www.hhs.gov/pandemicflu/plan/sup6.html and http://www.hhs.gov/pandemicflu/plan/sup7.html.
☐	☐	☐	Encourage and track seasonal influenza vaccination for employees every year. See www.cdc.gov/flu/protect/preventing.htm. Encourage all employees and their families to be up-to-date on all adult and child vaccinations recommended by the Advisory Committee on Immunization Practices. See www.cdc.gov/nip/recs/adult-schedule.htm and www.cdc.gov/nip/recs/child-schedule.htm.
☐	☐	☐	Evaluate employee access to and availability of health care, mental health, social services, community, and faith-based resources during a pandemic, and improve services as needed. See www.hhs.gov/pandemicflu/plan/sup11.html.

Plan for providing services to the public during a pandemic

Completed	In Progress	Not Started	
☐	☐	☐	Identify community-based scenarios and needs likely to occur in a pandemic emergency, and plan how to respond. These might include security of health care and/or vaccine distribution sites, sites that store antiviral medications or vaccines, first-responder activities, protection of critical infrastructure, management of panic and/or public fear, crowd/riot control, enforcement of public health orders, etc.
☐	☐	☐	Develop traffic flow plans to deal with standard traffic management and traffic flow around health-care delivery sites, including vaccine and antiviral distribution sites
☐	☐	☐	Anticipate community vulnerabilities (vulnerable populations, crimes of opportunity, fraudulent schemes, etc.) and specifically train employees to respond.
☐	☐	☐	Develop guidance for managing/assisting special populations (e.g., persons who are homeless, substance abusers, elderly, and individuals with disabilities, etc.) during a pandemic. This will require coordination with public health agencies, social services, correctional facilities, legal system representatives, and community-based organizations serving these populations.
☐	☐	☐	Work with local and/or State health departments or other relevant resources to ensure health protection and care for detainees or other individuals for whom the agency has responsibility.
☐	☐	☐	Establish policies on post-arrest management of an ill or exposed individual, including what to do should a care facility, precinct, and/or other law enforcement facility refuse entry to an ill or exposed individual.

3

Figure 11.39 (CONTINUED) Law enforcement pandemic influenza planning checklist from the CDC. (From HHS, Law enforcement pandemic influenza planning checklist, www.flu.gov/planning-preparedness/business/lawenforcement.pdf.)

(Continued)

Plan for coordination with external organizations and help your community

Completed	In Progress	Not Started	
☐	☐	☐	Review your pandemic influenza preparedness and response plan with key stakeholders inside and outside the agency, including employee representatives, and determine opportunities for collaboration, modification of the plan, and the development of complementary responsibilities.
☐	☐	☐	Share preparedness and response plans with other law enforcement agencies and law enforcement support agencies in your region or State (to include the National Guard) in order to share resources, identify collaboration strategies, and improve community response efforts. Develop, review, and modify local and State mutual aid agreements, if necessary. Mutual aid during an influenza pandemic can not be counted on as multiple jurisdictions in a given region may be affected simultaneously and have limited aid to offer. Availability of one State's National Guard to support another States plans under an existing compact (e.g., Emergency Management Assistance Compact) may be limited due to competing demands in their home State.
☐	☐	☐	Coordinate all requests for assistance with the next higher level governmental entity (e.g., local officials coordinate with State officials, State officials coordinate with Federal officials). Coordination is essential to ensure the assets: (1) can be provided in accordance with existing laws, (2) the requested resources are available. During a pandemic influenza, assistance from the next higher level of government may be limited due to competing higher priority demands and the effects of the influenza pandemic on these assets.
☐	☐	☐	Integrate planning with emergency service and criminal justice organizations such as courts, corrections, probation and parole, social services, multi-jurisdictional entities, public works, and other emergency management providers (fire, EMS, mutual aid, etc.).
☐	☐	☐	States should plan on utilizing their National Guard to perform law enforcement and security functions during a pandemic influenza. The National Guard under the command and control of the respective State's Governor is not subject to Posse Comitatus Act restrictions as are Federal military forces. Availability of one State's National Guard to support another States plans under an existing compact (e.g., Emergency Management Assistance Compact) may be limited due to competing demands in their home State.
☐	☐	☐	Security functions are essential during a pandemic influenza. Through your city or county attorney, corporation counsel or other appropriate authority, collaborate with the Office of the State Attorney General to clarify and review the authorities granted to law enforcement to include the National Guard. Suggest clarifications and work arounds as needed, and integrate into agency policy, training, and communications activities.
☐	☐	☐	Identify local or regional entities, such as health-care agencies, community organizations, businesses, or critical infrastructure sites, to determine potential collaboration opportunities. This collaboration might involve situational awareness, exercises or drills, or public safety training.
☐	☐	☐	Collaborate with local and/or State public health agencies to assist with the possible investigation of contacts within a suspected outbreak, the enforcement of public health orders, as well as the provision of security, protection, and possibly, critical supplies to quarantined persons. Each law enforcement agency will need to interact with local, State, county, and tribal public health officials to define the extent of the authorities provided from State legislation, develop procedures for the local initiation, implementation, and use of those authorities, as well as define protections from liability for law enforcement that may arise from quarantine and isolation enforcement. Operational planning must be flexible enough to address all scenarios in an all hazards environment, and in light of emerging infectious diseases.

Figure 11.39 (CONTINUED) Law enforcement pandemic influenza planning checklist from the CDC. (From HHS, Law enforcement pandemic influenza planning checklist, www.flu.gov/planning-preparedness/business/lawenforcement.pdf.)

Homeland Security

Pandemic planning and preparedness need occur during periods of “calm,” when strategic planning is clear and free from the intensity of the moment.⁵¹

Internet Exercise: HHS has produced a bevy of materials that anticipate the prevention as well as impact of a pandemic. See <https://www.cdc.gov/flu/prevent/index.html>.

11.4.3 Response and Recovery under COVID-19

Given the magnitude of the COVID-19 outbreak, being the largest pandemic challenge since 1918, the amount of advice regarding response and recovery has reached legendary proportions. Advice is everywhere, and while we have become accustomed to “Hand-Washing” as well as the use of “Masks” and been exhorted to isolate and social distance from one another, the list of particular response advice goes on perpetually. See Figure 11.40.

FEMA, by way of example, publishes Fact Sheets, covering a plethora of topics. See Figure 11.41.⁵²

DHS authors and disseminates response advice on many topics which in turn hopes to prevent the spread of this awful virus. One of its best efforts is its “Weekly Update”—an example reproduced at Figure 11.42.⁵³

Health and Human Services is spearheading the program Operation Warp Speed which seeks to accelerate normal times for vaccine development. The full description of this program is at Figure 11.43.⁵⁴

All of these responses are representative of steps each constituency needs of will take. Whether the Department of Education or the Department of Defense, every entity of government has a COVID-19 response and recovery plan. The challenge is in halting its spread and assuring a return to a greater normalcy than witnessed the last year.

11.5 Conclusion

This chapter deals with the public health dimensions of the homeland security problem. Biotoxins and bioterrorism must weigh heavily on the minds of those entrusted with minimizing the effects of these and other threats. DHS fully understands the potential for massive public health risk and injury. Working closely with the EPA, HHS, the USDA, and the Department of the Interior, DHS looks for those actions that might cause extensive public harm in a health context. Hence, water, its facilities and corresponding security, and threat assessment plans receive significant attention.

Equally important will be potential threats against our agricultural and food supplies. That contamination of the food chain would be an extraordinary public health dilemma cannot be overemphasized. Farm installations must also dwell on secured practices to ensure integrity in the food chain. Diseased animals represent a threat too. Featured within the chapter is the infectious animal disease facility at Plum Island in the waters near Rhode Island and New York. The SPPA highlights and targets the most common threats to the agricultural marketplace and its providers. Just as crucial in the homeland defense of our agricultural infrastructure is the inspection plan of facilities by the USDA. Special attention is given to the massive COVID-19 outbreak currently beleaguering the entire United States. The virus is reviewed from its Chinese inception, its spread and contagiousness in Europe and how New York City became its ultimate epicenter. Strategies to mitigate, remediate, respond and recover are fully analyzed. Finally, the chapter introduces the health dimensions of biological agents as threats to public health, the role of medical facilities in terms of response, and the particular strategies for agents.

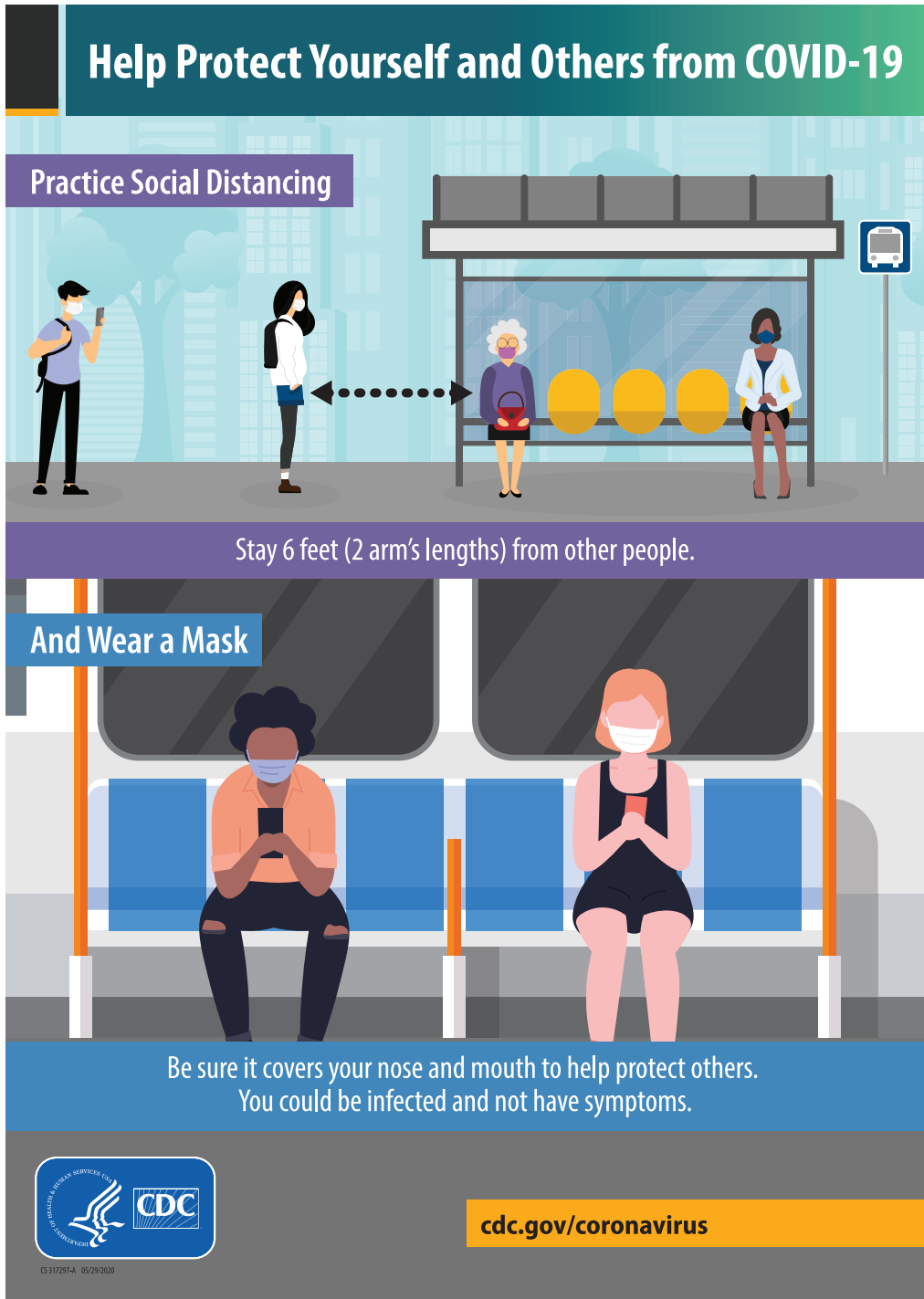


Figure 11.40 Illustration of social distancing. (Source: CDC.)



Navigation

Search

Languages

Coronavirus (COVID-19) Response
 Patients & Healthcare Workers
 State, Local, Tribal & Territorial Governments
 Economic Support & Recovery
 Understanding Data & Prioritizing Resources
 News & Media Gallery
 News Releases
 Regional News Releases
 Blogs
 Disaster Declarations
 Fact Sheets & Guidance
 Media Gallery
 How to Help
 Rumor Control
 Coronavirus Best Practices
 FEMA Careers

COVID-19 Fact Sheets & Guidance

Multimedia Home

News Releases

Disaster Declarations

Media Gallery



[Español](#) | [Haitian Creole](#)

View the most recent fact sheets and guidance documents related to the COVID-19 response.

Expand All Sections

Fact Sheets

- Respirators for Healthcare during COVID-19: Authorized Use and Avoiding Fraudulent Products ([English](#)) | July 8, 2020
- Coordinating Public Assistance and Other Sources of Federal Funding ([English](#)) | July 1, 2020
- Historic Preservation Compliance for Emergency Protective Measures ([English](#)) ([Spanish](#)) ([Haitian Creole](#)) | June 5, 2020
- Exercise Starter Kit for Preparedness in a Pandemic ([English](#)) | June 1, 2020
- Distribution of Infrared Thermometers ([English](#)) ([Spanish](#)) | May 26, 2020
- Community Mitigation Decision Support Tool ([English](#)) | May 22, 2020
- Supply Chain Expansion Line of Effort ([English](#)) | May 18, 2020
- Alternate Care Site (ACS) "Warm Sites" ([English](#)) ([Spanish](#)) | May 12, 2020

Figure 11.41 FEMA's COVID-19 Fact Sheet.

Official website of the Department of Homeland Security

Contact Us | Quick Links | Site Map | A-Z Index

Homeland Security

Topics | News | In Focus | How Do I? | Get Involved | About DHS

Enter Search Term | On DHS.gov | Search

News > Press Releases > Weekly Update: DHS Response to COVID-19

Weekly Update: DHS Response to COVID-19

Release Date: June 22, 2020

The Department of Homeland Security remains vigilant against the COVID-19 virus and continues to lead the national response to minimize the impact of COVID-19 on American citizens and workers. As the nation transitions to a phased approach of reopening the economy the Department and its components remain steadfast in their commitment to ensure a safe, secure, and prosperous Homeland for the American people.

"S&T has dedicated its research acumen to addressing the needs of the pandemic response efforts with actionable science-based, information," said William N. Bryan, DHS Senior Official Performing the Duties of the Under Secretary for Science & Technology. "We began research at the very beginning of the outbreak to determine what was known about the virus, and determined what else we needed to know in order to control the spread. Our efforts have discovered how temperature, humidity, and especially sunlight, can help to limit the spread of the virus from surfaces and in the air. We've determined effective decontamination methods for cleaning surfaces with simple household chemicals, and just this week, released information about how to use a multicooker to decontaminate critical PPE, such as N95 masks, for reuse. I am proud of S&T's team and our abilities to contribute to the global response efforts to control the spread of this deadly disease."

Below is a list of some of DHS's efforts against COVID-19 last week:

Science and Technology (S&T)

Delivering Actionable Information Through Applied Research. Personal protective equipment, specifically respiratory protection such as N95 masks, are an effective way to reduce exposure to airborne SARS-CoV-2, the coronavirus that causes COVID-19. With high demand resulting in limited supply, S&T focused efforts on finding affordable and easy methods that allow masks to safely be reused. On June 19th, S&T [published](#) information about using a multi-cooker as an effective low-technology decontamination option for N95 respirators. A fact sheet, question-and-answer document, concept of operations, and an [instructional video](#) were posted on S&T's website for easy access to the information.

Driving Evidence-Based Policymaking. On June 16th, Science and Technology updated its [Master Question List](#) (MQL), a compilation of available research on operationally relevant questions to aid decision makers in the COVID-19 response. The MQL is a quick-reference guide covering what is known about the virus, what additional information is needed, and who may be working to address these fundamental questions. New entries include references to

Figure 11.42 DHS's COVID-19 Weekly Update.



Explaining Operation Warp Speed

What's the goal?

Operation Warp Speed (OWS) aims to deliver 300 million doses of a safe, effective vaccine for COVID-19 by January 2021, as part of a broader strategy to accelerate the development, manufacturing, and distribution of COVID-19 vaccines, therapeutics, and diagnostics (collectively known as countermeasures).

How will the goal be accomplished?

By investing in and coordinating countermeasure development, OWS will allow countermeasures such as a vaccine to be delivered to patients more rapidly while adhering to standards for safety and efficacy.

Who's working on it?

OWS is a partnership among components of the Department of Health and Human Services (HHS), including the Centers for Disease Control and Prevention (CDC), the Food and Drug Administration (FDA), the National Institutes of Health (NIH), and the Biomedical Advanced Research and Development Authority (BARDA), and the Department of Defense (DoD). OWS engages with private firms and other federal agencies, including the Department of Agriculture, the Department of Energy, and the Department of Veterans Affairs. It will coordinate existing HHS-wide efforts, including the NIH's Accelerating COVID-19 Therapeutic Interventions and Vaccines (ACTIV) partnership, NIH's Rapid Acceleration of Diagnostics (RADx) initiative, and work by BARDA.

What's the plan and what's happened so far?

DEVELOPMENT: To accelerate development while maintaining standards for safety and efficacy, OWS has been selecting the most promising countermeasure candidates and providing coordinated government support.

Protocols for the demonstration of safety and efficacy are being aligned, which will allow the trials to proceed more quickly, and the protocols for the trials will be overseen by the federal government, as opposed to traditional public-private partnerships, in which pharmaceutical companies decide on their own protocols. Rather than eliminating steps from traditional development timelines, steps will proceed simultaneously, such as starting manufacturing of the vaccine at industrial scale well before the demonstration of vaccine efficacy and safety as happens normally. This increases the financial risk, but not the product risk.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES | PAGE 1

Figure 11.43 Operation Warp Speed (OWS) aimed to initially deliver tens of millions, then hundreds of millions, of doses of a safe, effective vaccine for COVID-19 to be rolled out in a coordinated effort in 2021.

(Continued)

Explaining Operation Warp Speed

Select actions to support OWS vaccine development so far include:

- March 30: HHS [announced](#) \$456 million in funds for Johnson & Johnson's candidate vaccine, with Phase 1 clinical trials set to begin this summer.
- April 16: HHS [made](#) up to \$483 million in support available for Moderna's candidate vaccine, which began Phase 1 trials on March 16 and received a fast-track designation from FDA.
- May 21: HHS [announced](#) up to \$1.2 billion in support for AstraZeneca's candidate vaccine, developed in conjunction with the University of Oxford. The agreement is to make available at least 300 million doses of the vaccine for the United States, with the first doses delivered as early as October 2020 and Phase 3 clinical studies beginning this summer with approximately 30,000 volunteers in the United States.

[As announced](#) on May 15, the vaccine development plan is as follows, subject to change as work proceeds:

- Fourteen promising candidates have been chosen from the 100+ vaccine candidates currently in development—some of them already in clinical trials with U.S. government support.
- The 14 vaccine candidates are being narrowed down to about seven candidates, representing the most promising candidates from a range of technology options, which will go through further testing in early-stage clinical trials.
- Large-scale randomized trials for the demonstration of safety and efficacy will proceed for the most promising candidates.

MANUFACTURING: The federal government is making investments in the necessary manufacturing capacity at its own risk, giving firms confidence that they can invest aggressively in development and allowing faster distribution of an eventual vaccine. Manufacturing capacity for selected candidates will be advanced while they are still in development, rather than scaled up after approval or authorization. Manufacturing capacity developed will be used for whatever vaccine is eventually successful, if possible given the nature of the successful product, regardless of which firms have developed the capacity.

Select actions to support OWS manufacturing efforts so far include:

- The May 21, April 16, and March 30 HHS agreements with AstraZeneca, Moderna, and Johnson & Johnson respectively include investments in manufacturing capabilities.
- June 1: HHS [announced](#) a task order with Emergent BioSolutions to advance domestic manufacturing capabilities and capacity for a potential COVID-19 vaccine as well as therapeutics, worth approximately \$628 million.

DISTRIBUTION: Before the countermeasures are approved or authorized, the program will build the necessary plans and infrastructure for distribution.

HHS plans for a tiered approach to vaccine distribution, which will build on allocation methodology developed as part of pandemic flu planning and be adjusted based on experience

Figure 11.43 (*CONTINUED*) Operation Warp Speed (OWS) aimed to initially deliver tens of millions, then hundreds of millions, of doses of a safe, effective vaccine for COVID-19 to be rolled out in a coordinated effort in 2021.

(Continued)

Explaining Operation Warp Speed

during the first wave of the COVID-19 response, data on the virus and its impact on populations and the performance of each vaccine, and the needs of the essential workforce. OWS will expand domestic manufacturing and supplies of specialized materials and resources, such as glass vials, that can be necessary for distribution. DoD's involvement will enable faster distribution and administration than would have otherwise been possible.

Select actions to support OWS distribution efforts include:

- May 12: DoD and HHS [announced](#) a \$138 million contract with Apixect for more than 100 million prefilled syringes for distribution across the United States by year-end 2020, as well as the development of manufacturing capacity for the ultimate production goal of over 500 million prefilled syringes in 2021.
- June 9: HHS and DoD announced a joint effort to increase domestic manufacturing capacity for vials that may be needed for vaccines and treatments:
 - \$204 million to Corning to expand the domestic manufacturing capacity to produce an additional 164 million Valor Glass vials each year if needed.
 - \$143 million to SiO₂ Materials Science to ramp up capacity to produce the company's glass-coated plastic container, which can be used for drugs and vaccines.

Who's leading OWS?

HHS Secretary Alex Azar and Defense Secretary Mark Esper oversee OWS, with Dr. Moncef Slaoui designated as chief advisor and General Gustave F. Perna nominated to be chief operating officer. To allow these OWS leaders to focus on operational work, in the near future the program will be announcing separate points of contact, with deep expertise and involvement in the program, for communication with Congress and the public.

What are you doing to make these products affordable for Americans?

As a commitment to making countermeasures affordable for the American people, and as a condition of receiving support from OWS, companies will provide to the U.S. government an allocation of countermeasures developed.

How is this being funded?

Congress has directed almost \$10 billion to this effort through supplemental funding, including the CARES Act. Congress has also appropriated other flexible funding. The almost \$10 billion specifically directed includes more than \$6.5 billion designated for countermeasure development through BARDA and \$3 billion for NIH research.

Figure 11.43 (*CONTINUED*) Operation Warp Speed (OWS) aimed to initially deliver tens of millions, then hundreds of millions, of doses of a safe, effective vaccine for COVID-19 to be rolled out in a coordinated effort in 2021.

Homeland Security

Keywords

Agroterrorism; Animal and Plant Health Inspection; Service; Assessment Protocol; Avian Flu; Bioterrorism; Bird Flu; Chemical Agent; Communicable Disease; Contamination; COVID-19; Department of Agriculture; Environmental Protection Agency; Epidemic; Food Safety and Inspection Service; Food Safety Officer; H5N1; Hospital Preparedness Program; Import Surveillance Liaison Officer; Infectious Disease; Influenza; Mad Cow Disease; National Select Agency Registry Program; Pandemic; Pandemic Flu; Pathogen; Project BioShield; Seasonal Flu; Strategic Partnership Program On; Agroterrorism; Strategic National Stockpile; Swine Flu; Virus; Water Security Division; World Health Organization

Discussion Questions

1. In what way do federal and state agencies deal with water and its protection?
2. What role do hospitals play in questions of homeland defense and public health?
3. Explain how the food chain can be compromised.
4. Explain how biotoxins can cause massive damage to the public health. Give specific examples.
5. Why does DHS rely so heavily on the USDA in public health planning?
6. Relate the purpose and aim of Project BioShield.
7. With the rise of medicine and clinical intervention, will a pandemic be more or less likely?

Practical Exercises

1. Visit the EPA's water security home at <http://water.epa.gov/infrastructure/watersecurity/index.cfm>. Click on and research their various water security tools.
2. Envision how the food production cycle affords the terrorist opportunity. How could this be so? Author a hypothetical fact pattern that shows how food production may oddly be a forum for the terrorist.
3. Animals and plants may also afford the terrorist threat and terror opportunities. Relate four potential scenarios where this might occur.
4. Contact your state homeland security agency. Find out about pandemic preparedness and recovery.
5. Review the Biden COVID-19 Fact Sheet from January 15, 2021.

<https://www.whitehouse.gov/briefing-room/statements-releases/2021/01/15/fact-sheet-president-elect-biden-outlines-covid-19-vaccination-plan/>

Take one aspect from it and research how effectively and accurately it was carried out in actuality.

Notes

- 1 John Hopkins Coronavirus Resource Center, COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU), August 22, 2020, <https://coronavirus.jhu.edu/map.html> (accessed November 30, 2020).
- 2 All of these activities conjure up devastation and fear in the populace. It will be crucial for government to address the magnitude of the potential harm while respecting the rule of law. See B. K. Collins and H. Morrow, Using shared technology in bioterrorism planning and response: Do privacy laws affect administrative judgments? *The Homeland Security Review*, 4 (2010): 43.
- 3 DHS, Critical infrastructure sectors, <http://www.dhs.gov/critical-infrastructure-sectors> (accessed August 22, 2020).
- 4 D. K. Stocker, P. Griffin, and C. Kocher, A functionalist's perspective on bioterrorism and global adversity, *The Homeland Security Review*, 4 (2010): 2.
- 5 Environmental Protection Agency, Information about Public Water Systems, <https://www.epa.gov/dwreginfo/information-about-public-water-systems> (accessed August 22, 2020).
- 6 EPA, Planning for an emergency drinking water supply (June 2011), http://www.epa.gov/sites/production/files/2015-03/documents/planning_for_an_emergency_drinking_water_supply.pdf (accessed August 22, 2020).
- 7 Environmental Protection Agency, Risk and Resilience Assessments and Emergency Response Plans, https://www.epa.gov/sites/production/files/2019-04/documents/awia_factsheet_04-16-2019_v2-508.pdf (accessed August 22, 2020); EPA, *Vulnerability Assessment Fact Sheet* (Washington, DC: U.S. Government Printing Office, 2002), EPA816-F-02-025.
- 8 See Congressional Research Service (CRS), *The Federal Food Safety System: A Primer* (Washington, DC: Library of Congress, January 11, 2011), <http://www.fas.org/sgp/crs/misc/RS22600.pdf> (accessed August 22, 2020).
- 9 UFW worker requirements and labor laws have been relaxed to assure a stream of workers. See: US Dept of Homeland Security, Press Release DHS and USDA Move to Protect American Farmers and Ensure Continued Flow of America's Food Supply, April 15, 2020, <https://www.dhs.gov/news/2020/04/15/dhs-and-usda-move-protect-american-farmers-and-ensure-continued-flow-america-s-food> (accessed August 22, 2020).
- 10 CDC, Morbidity and Mortality Weekly Report, COVID-19 Among Workers in Meat and Poultry Processing Facilities — 19 States, April 2020 (May 8, 2020), <https://www.cdc.gov/mmwr/volumes/69/wr/mm6918e3.htm> (accessed August 22, 2020).
- 11 Ibid at Table 2.
- 12 FDA, *Risk Assessment for Food Terrorism and Other Food Safety Concerns* (Silver Spring, MD: FDA, 2003), <https://seafood.oregonstate.edu/sites/agscid7/files/snic/risk-assessment-for-food-terrorism-and-other-food-safety-concerns.pdf> (accessed August 22, 2020).
- 13 USDA, DHS, and FDA, *Critical Infrastructure and Key Resources for Sector Specific Plan as Input to the National Infrastructure Protection Plan* (Washington, DC: U.S. Government Printing Office, 2007), 2.
- 14 USDA, *Pre-Harvest Security Guidelines and Checklist 2006* (Washington, DC: U.S. Government Printing Office, 2006), 3, <https://www.hsdl.org/?abstract&did=465011> (accessed August 22, 2020).
- 15 CISA, Food and Agriculture Sector Website, <https://www.dhs.gov/food-and-agriculture-sector> (accessed August 22, 2020); See also: FSIS, Food Defense Training Module at May 31, 2020, https://www.fsis.usda.gov/wps/wcm/connect/621ce985-9691-44e9-b3c2-9c8fbd961cc1/PHVt-Homeland_Food_Defense.pdf?MOD=AJPERES (accessed August 22, 2020).
- 16 USDA, *Pre-Harvest Security Guidelines*, 10–11.
- 17 D. K. Stocker, P. M. Griffin, C.J. Kocher, and T. M. Raquet, Agroterrorism: Risk assessment and proactive responses, *The Homeland Security Review*, 5 (2011): 17. See also: K. Govern, Agroterrorism and eco-terrorism: A survey of Indo-American approaches under law and policy to prevent and defend against these potential threats ahead, *Florida Coastal Law Review*, 10 (2009): 223.
- 18 FDA, Strategic Partnership Program Agroterrorism (SPPA) initiative, <http://www.fda.gov/Food/FoodDefense/FoodDefensePrograms/ucm080836.htm> (accessed August 22, 2020).

Homeland Security

- 19 FDA, Vulnerability Assessments of Food Systems: June 2009–February 2012, 4 (2012), <https://www.fda.gov/media/84376/download> (accessed August 22, 2020); U.S. Food and Drug Administration, Strategic Partnership Program Agroterrorism (SPPA) Initiative: Final Summary Report September 2005–September 2008 (2008), Appendix A, <https://www.fda.gov/food/food-defense-programs/strategic-partnership-program-agroterrorism-sppa-initiative-second-year-status-report-july-2006> (accessed August 22, 2020).
- 20 FDA, Vulnerability Assessments of Food Systems, at 5.
- 21 Stocker, Griffin, Kocher, and Raquet, Agroterrorism, 17, 20.
- 22 Dept of Homeland Security, Plum Island Animal Disease Center, https://www.dhs.gov/sites/default/files/publications/plum_island_animal_disease_center-piadc-12132019.pdf (accessed August 22, 2020).
- 23 USDA, Agricultural Research Service, “Northeast area research projects,” http://www.ars.usda.gov/main/site_main.htm?modecode=80-00-00-00 (accessed August 22, 2020).
- 24 US Dept of Agriculture, Virulent Newcastle Disease Flyer, https://www.aphis.usda.gov/publications/animal_health/fsc-vnd-know-signs.pdf (accessed August 22, 2020).
- 25 See CRS, *Federal Efforts to Address the Threat of Bioterrorism: Selected Issues and Options for Congress* (Washington, DC: Library of Congress, February 8, 2011), <http://www.fas.org/sgp/crs/terror/R41123.pdf> (accessed August 22, 2020). For examples of experts who downplay the threat posed by bioterrorism, see M. Leitenberg, *Assessing the Biological Weapons and Bioterrorism Threat*, Strategic Studies Institute, U.S. Army War College; Scientists Working Group on Biological and Chemical Weapons, Center for Arms Control and Non-Proliferation, *Biological Threats: A Matter of Balance*, January 26, 2010; Scientists Working Group on Biological and Chemical Weapons, Biological threats: A matter of balance, *Bulletin of the Atomic Scientists*, February 2, 2010.
- 26 See CRS, *Federal Efforts*, 8–9.
- 27 CDC, National Notifiable Diseases Surveillance System, 2020 National Notifiable Infectious Diseases, <https://wwwn.cdc.gov/nndss/conditions/notifiable/2020/infectious-diseases> (accessed August 22, 2020).
- 28 See J. Tropper, C. Adamski, C. Vionion, and S. Sapkota, Tracking antimicrobials dispensed during an anthrax attack: A case study from the New Hampshire anthrax exercise, *Journal of Emergency Management*, 9 (January/February 2011): 65.
- 29 CDC, Emergency preparedness and response: Bioterrorism overview, <https://emergency.cdc.gov/bioterrorism/> (accessed August 22, 2020).
- 30 Project BioShield Act of 2004, P.L. 108–276, *U.S. Statutes at Large*, 118 (2004): 835.
- 31 For an update on BioShield’s many activities, see Robert Kadlec, *Renewing the Project BioShield Act: What Has It Bought and Wrought?* (Policy brief) (Washington, DC: Center for a New American Security, 2013), <https://www.cnas.org/publications/reports/renewing-the-project-bioshield-act-what-has-it-bought-and-wrought> (accessed August 22, 2020); CRS, *Project BioShield: Authorities, Appropriations, Acquisitions, and Issues for Congress* (Washington, DC: CRS, May 27, 2011), <http://www.fas.org/sgp/crs/terror/R41033.pdf> (accessed August 22, 2020).
- 32 Medical Countermeasures.gov, BARDA Coronavirus Response, <https://www.medicalcountermeasures.gov/home.aspx> (accessed August 22, 2020).
- 33 Public Health Emergency.gov, HHS/ASPR Strategic National Stockpile- Response to the COVID-19 Pandemic, <https://www.phe.gov/emergency/events/COVID19/SNS/Pages/default.aspx> (accessed August 22, 2020).
- 34 There are even more legal issues and potential liabilities associated with pandemics when compared with other natural disasters. See B. Courtney, Five legal preparedness challenges for responding to future public health emergencies, *Journal of Law, Medicine & Ethics* (Spring 2011): 60.
- 35 CDC, Variant Influenza Viruses: Background and CDC Risk Assessment and Reporting, <https://www.cdc.gov/flu/swineflu/variant.htm> (accessed August 22, 2020).
- 36 CDC, The burden of the influenza A H1N1pdm09 virus since the 2009 pandemic, <https://www.cdc.gov/flu/pandemic-resources/burden-of-h1n1.html> (accessed August 22, 2020).
- 37 CDC, PandemicFlu.gov, <http://pandemicflu.gov/general/index.html> (accessed August 22, 2020).
- 38 WHO, *Pandemic Influenza Preparedness and Response: A WHO Guidance Document* (Washington, DC: U.S. Government Printing Office, 2009).
- 39 See: Family Research Council, Coronavirus Deception: Made in China, (May 6, 2020), <https://www.frc.org/updatearticle/20200506/coronavirus-deception> (accessed August 22, 2020).

- 40 See: Walter Russell Mead, China Still Misleads the World on Coronavirus, Wall Street Journal, April 13, 2020, <https://www.wsj.com/articles/china-still-misleads-the-world-on-the-coronavirus-11586818132> (accessed August 22, 2020).
- 41 New York City Dept of Health, COVID-19: Data, <https://www1.nyc.gov/site/doh/covid/covid-19-data-deaths.page> (accessed August 22, 2020).
- 42 Benedict Carey and James Glanz, Travel from New York City Seeded Wave of U.S. Outbreaks, *The New York Times*, May 7, 2020, <https://www.nytimes.com/2020/05/07/us/new-york-city-coronavirus-outbreak.html> (accessed August 22, 2020).
- 43 Ibid.
- 44 CDC, Coronavirus Disease 2019 (COVID-19) Cases in the US, <https://www.cdc.gov/coronavirus/2019-ncov/cases-updates/cases-in-us.html> (accessed August 22, 2020).
- 45 See: D. Estrin, After Reopening Schools, Israel Orders Them to Shut If COVID-19 Cases Are Discovered, NPR, June 3, 2020, <https://www.npr.org/sections/coronavirus-live-updates/2020/06/03/868507524/israel-orders-schools-to-close-when-covid-19-cases-are-discovered> (accessed August 22, 2020).
- 46 For general advice on the preparedness model, see WHO, Pandemic influenza preparedness: Sharing of influenza viruses and access to vaccines and other benefits, 63rd World Health Assembly, Provisional agenda item 11.1 (April 2010), http://apps.who.int/gb/ebwha/pdf_files/WHA63/A63_4-en.pdf (accessed August 22, 2020); See also WHO, Regional pandemic influenza preparedness and response plan, 2009–2010 (May 2009), https://www.who.int/influenza/resources/documents/pandemic_guidance_04_2009/en/ (accessed August 22, 2020); J. R. Langabeer II and J. L. DelliFraine, Incorporating strategic management into public health emergency preparedness, *Journal of Emergency Management*, 9 (March/April 2011): 17; See also: https://www.cdc.gov/flu/pandemic-resources/pdf/pandemic-influenza-implementation.pdf?fbclid=IwAR0L2Mdh6-pwWYpDQ_pcvSRWRM6T772WNTqGfIp2pk9G2nm6ahP2d-2VsOc (accessed August 22, 2020).
- 47 World Health Organization, WHO Coronavirus Disease (COVID-19) Dashboard, August 22, 2020, https://covid19.who.int/?gclid=EAIaIQobChMIs-KExqGd6gIVjYnICh2JYgGhEAAAYASABEgL-haPD_BwE (accessed August 22, 2020).
- 48 DHS, *Pandemic Influenza: Preparedness, Response and Recovery Guide for Critical Infrastructure and Key Resources* (Washington, DC: DHS, 2006), <http://www.flu.gov/planning-preparedness/business/cikrpandemicinfluenzaguide.pdf> (accessed August 22, 2020).
- 49 HHS, *HHS Pandemic Influenza Plan: Part 1; Strategic Plan* (Washington, DC: HHS), <https://scholarworks.iupui.edu/handle/1805/860> (accessed August 22, 2020). See also: FEMA, *Continuity of Operations: An Overview of Continuing Planning for Pandemic Influenza* (Washington, DC: FEMA, 2011), http://www.fema.gov/pdf/about/org/ncp/pandemic_influenza.pdf (accessed August 22, 2020).
- 50 Dept of Health and Human Services, Law Enforcement Pandemic Influenza Planning Checklist, <https://espanol.cdc.gov/flu/pandemic-resources/pdf/lawenforcement.pdf> (accessed August 22, 2020); G. Waight et al., The role of medical students in influenza pandemic response, *Journal of Emergency Management*, 9 (March/April 2011): 60.
- 51 J. R. Langabeer II and J. L. DelliFraine, Incorporating strategic management into public health emergency preparedness, *Journal of Emergency Management*, 9 (March/April 2011): 17, 25.
- 52 FEMA, COVID-19 Fact Sheets & Guidance Webpage, <https://www.fema.gov/coronavirus/fact-sheets> (accessed August 22, 2020).
- 53 US Dept. of Homeland Security, Weekly Update: DHS Response to COVID-19, <https://www.dhs.gov/news/2020/06/22/weekly-update-dhs-response-covid-19> (accessed August 22, 2020).
- 54 US Dept of Health and Human Services, Explaining Operation Warp Speed Fact Sheet, <https://www.hhs.gov/sites/default/files/fact-sheet-operation-warp-speed.pdf> (accessed August 22, 2020).



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

The Future of Homeland Security

12.1 Introduction

In the past 20 years, the Department of Homeland Security (DHS) has evolved in dramatic ways—in both a bureaucratic and a mission sense. The fact that this agency was born with such speed, and that it subsequently metamorphosed into a full-blown department, is testimony to its unique nature in the world of government. Nothing moves all that quickly in the worlds of bureaucracy and government entities although DHS appears to have broken the sound barrier. Given this pace of establishment and growth, it is valid to question whether there is consensus on exactly what *homeland security* even is. The fact that there are hundreds, even thousands, of initiatives in homeland defense proves very little about their universal relevance to what might be described as *core missions*. Shortly after 9/11, it seems improbable that livestock, corn, avian and swine flu, COVID-19, the Internet and the cyber domain, as well as telecommunications, would be the vernacular and purview of the homeland initiative. Prior to 9/11, the principles and practices of homeland defense were rather narrowly constructed.

Today there is the constant, real danger of mission creep. Some entities outside and within the government have convinced themselves that areas that seem far afield from homeland security have direct connections to the homeland security universe. Thinking broadly, just about every human activity could fall under the homeland security umbrella. In some cases this would be right; in other cases, this would be wrong and even counterproductive. Some of these “wrong” choices are often to the detriment of citizens’ privacies and civil liberties granted in the Constitution. Security is clearly of prime importance, but we must tread lightly.

DHS as currently constructed and operated still has the capacity to jump on any new program initiative that it can invent or that someone can imagine. In short, DHS has never met a program it did not like (or could not rationalize). While the administrators and operatives within DHS may not intend this, the operational life-form of DHS plays and feeds on fear itself, to the tune of billions of taxpayer’s dollars. Strategists and policymakers bandy about every imaginable solution, while fear of the unknown event, plot, or disaster hangs like a specter over every decision. DHS cannot protect every citizen in every quarter, in every situation. DHS cannot possibly design and divine policy for every facet of human life.

Today, there is equally the danger of mission confusion to the point of chaos. In multiple quarters of the dialogue, there is a strong divergence of opinions on whom and why terrorism exists or is defined and how to defend against them. On the one hand, climate change is the most serious challenge of our time, yet on the other hand, there are more immediate tragedies that take place and consume national attention and DHS resources. With the potential widespread and global environmental repercussions, does climate change outstrip the severity and devastation

Homeland Security

of nuclear bombs or weapons of mass destruction? At Fort Hood and at the San Bernadino shootings of November 2015, or the Saudi pilot training in Pensacola in 2019, who shot American naval pilots, exclaiming “Allahu Akbar” prior to their acts, can we ignore any potential connection between radical Islamic fundamentalism and the events that occurred? There needs to be recognition that increasing self-radicalization throughout the world, including within the United States, is directly tied to Islamic extremist propaganda available online. In addition, the events of January 6th show that home-grown terrorism from white-nationalist and far-right groups is a real and growing threat to our democracy.

Even the employees of DHS, fully surveyed in 2015, manifest a current lack of confidence in both the leadership and direction of the agency.¹ In a phrase, both mission creep and mission confusion undermine employee morale and esprit de corps. When former DHS director, Jeh Johnson, indicated he is concerned with the privacy rights of foreign terrorists and, as a result, does not feel it proper to check their activities on social media, you have some questionable policy decision-making coming from the top. Or when some DHS Directors failed to be vigilant on threats and to be caught flat-footed when disaster or catastrophe occurs, the agency trembles just a bit. On top of this, DHS, under the Presidency of Donald Trump, had rattled the agency with constant DHS Director changes, nearly five in 4 years. No agency can plant its feet and find its way in such turmoil of leadership. Hopefully the Biden administration’s choice Alejandro Mayorkas can bring some vision, stability, and consistency to the role and department.

Turning to the academic sector, even among colleges and universities, there is a lack of intellectual and conceptual consensus on what the homeland curriculum should be and what the homeland student should study. As Dr. William Pelfrey Sr. cogently argues:

Unfortunately, there is no clear roadmap to homeland security nor is there a consensus on appropriate curricula for homeland security programs. A review of federal publications on homeland security is dizzying. A myriad of Presidential Directives, Department of Homeland Security Publications, commission reports, and other publications leaves most academics and practitioners with their heads spinning.²

The academic debate also reflects the endless growth of various constituencies in seeking a piece or part of the homeland security pie since the early days after 9/11. As DHS talks about unification, efficiency, and universal mission, there should be concern about the notion of trying to be all things to all people.

DHS has placed itself in the tenuous position of being a guarantor in all aspects of human activity and interchange. As an example, one of the most difficult man-made tragedies to thwart is active shooter scenarios. Lone-wolf shooting events such as the July 2012 Aurora, Colorado, movie theater shooting that killed 12; the August 2012 shooting at a Sikh temple in Oak Creek, Wisconsin, that killed six; and the unspeakable shooting of 26 innocent children, teachers, and school administrators at Sandy Hook Elementary School in Newtown, Connecticut, or Parkland High School in Florida is only increasing in frequency.³

To be sure, our nation is beset by violent activities at every sector and locale imaginable, from wealthy suburbs to gang shootings in the streets in Chicago. In other words, with dozens of murders taking place weekly in Chicago or New York City, or the Black Lives Matter (BLM) protests and conflicts and, often violent, crackdown of local police and national police forces deployed by the Trump White House in both Portland, Oregon and in Lafayette Square in Washington D.C. in the summer of 2020, homeland security cannot lose sight of its ultimate purpose—to provide a safe environment for this country. Looked at another way, our own internal violence is causing us to miss what may be a homeland security catastrophic event. Active shooters alone are arresting our attention from things that assure the safety and tranquility of our homeland. From 2000 to 2018, the array of active shooter events continued its upward and seemingly inevitable rise, as the FBI charts in Figure 12.1.⁴

And the rise of this form of violence, sometimes jihadi driven, sometimes perpetrated by white nationalist groups—at other times the product of mental health breakdowns in individuals

Quick Look: 277 Active Shooter Incidents in the United States From 2000 to 2018

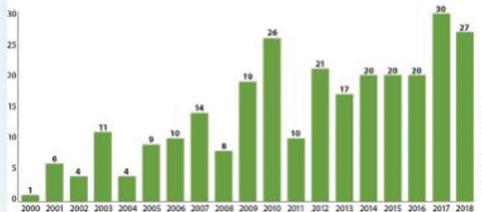
The five downloadable graphics below reflect statistical information pertaining to the 277 FBI-designated active shooter incidents that occurred in the United States from 2000 to 2018. These graphics depict the total number of incidents per year, total casualties per year, individuals killed and wounded per year, and incident locations. Click on each graphic for a higher resolution version. (Note: Authorization to reproduce these graphics is granted.)



The above map graphic contains a number of snapshot statistics of the active shooter incidents that occurred in the United States from 2000 to 2018. These statistics include 277 active shooter incidents and 2,430 casualties, including 884 killed and 1,546 wounded.

Quick Look: 277 Active Shooter Incidents in the United States Between 2000 - 2018

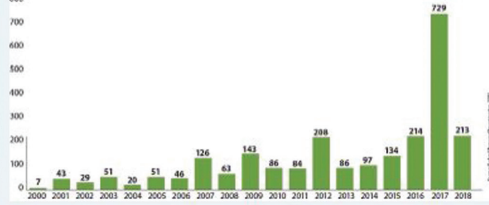
Incidents Per Year



The above bar chart contains the numbers of active shooter incidents in the United States, broken down by year, from 2000 to 2018. Those yearly numbers are: 2000, one incident; 2001, six incidents; 2002, four incidents; 2003, 11 incidents; 2004, four incidents; 2005, nine incidents; 2006, 10 incidents; 2007, 14 incidents; 2008, eight incidents; 2009, 19 incidents; 2010, 26 incidents; 2011, 10 incidents; 2012, 21 incidents; 2013, 17 incidents; 2014, 20 incidents; 2015, 20 incidents; 2016, 20 incidents; 2017, 30 incidents; and 2018, 27 incidents. The total number of active shooter incidents during the time frame was 277.

Quick Look: 277 Active Shooter Incidents in the United States Between 2000 - 2018

Casualties Per Year



The above bar chart contains statistics, broken down by year, of the number of casualties that resulted from active shooter incidents from 2000 to 2018. Those yearly numbers are: 2000, seven; 2001, 43; 2002, 39; 2003, 51; 2004, 20; 2005, 51; 2006, 46; 2007, 126; 2008, 63; 2009, 143; 2010, 86; 2011, 86; 2012, 208; 2013, 86; 2014, 97; 2015, 114; 2016, 214; 2017, 729; and 2018, 213. The total number of casualties for this time frame was 2,430.

Figure 12.1 Active Shooter incidents, charted from 2000 to 2018, show a steady rise.

and families—adds to the misunderstanding and real confusion in how to handle the challenges of homeland protection.

Indeed, our culture is now so plagued by political factions that we cannot even agree that terror is terror, or that radical Islamic fundamentalism is interconnected with terrorism. The lack of cohesion and sensibility as to purpose, terms, and outlook adds to the county's confused perceptions that other nations see from afar. The Fort Hood case cannot simply be written off as workplace violence given Major Hasan's deep ties to the jihadi movement. Nor can terms such as *misguided individuals* or *inappropriate gun violence* adequately or accurately describe the intense terror that the public experiences from attacks motivated wholly or in part by radical ideology. DHS has promised that food will be safe, that water will always be drinkable, that planes will never be hijacked, and that trains will never be derailed by terrorists. And yet, we still hear new reports of plots to smuggle explosives onto planes, the extremely costly expense, delays, and inability to finish the virtual or the actual fence initiative on the U.S.–Mexico border, and an aging U.S. power and utilities infrastructure that is subject to supervisory control and data acquisition (SCADA) and cyber-attacks. It is no wonder that the public is concerned about DHS's direction, mission, and focus. DHS must recognize and know, on some level, that it

Homeland Security

cannot do all. The Federal Emergency Management Agency (FEMA) seems to acknowledge this reality when it labels its current effort as *government centric*.

We fully recognize that a government-centric approach to emergency management is not enough to meet the challenges posed by a catastrophic incident. *Whole community* is an approach to emergency management that reinforces the fact that FEMA is only one part of our nation's emergency management team; that we must leverage all of the resources of our collective team in preparing for, protecting against, responding to, recovering from, and mitigating against all hazards; and that collectively we must meet the needs of the entire community in each of these areas.⁵

As DHS seeks to generate enthusiasm within the public, especially in publishing documents such as "One Team, One Mission, Securing the Homeland, 2008–2013,"⁶ the contents of the report paint a somewhat disappointing picture of half successes. In "Goal 1: Protect Our Nation from Dangerous People," arguably the central reason for the mission of DHS, the results by and large are mixed to poor no matter how you look at it (Figure 12.2).

Less than half of the air passengers with major violations of customs and immigration laws and regulations are apprehended. Just over one-third of vehicle travelers with major violations of customs and immigration laws and regulations are apprehended. The only true success story among those listed is that of the Coast Guard—an agency that remains mission oriented and does what it does exceedingly well. As exhibited by its response in the Haiti earthquake of 2011 and the BP oil spill, the last decades series and hurricanes and mass flooding, and per the Coast Guard's own posture statement for 2021, it is rightfully characterized as an entity that:

Our greatest value to the Nation resides in our ability to rapidly shift among our missions to meet national priorities during steady state and crisis. We will align all of our Service's initiatives to promote organizational efficiency, agility, and effectiveness – delivering excellence anytime, anywhere.⁷

Select Reported Measures for Goal 1: Protect Our Nation from Dangerous People	
Measure	FY 2013 Target
Border miles under effective control (including certain coastal sectors).	*
Air passenger apprehension rate for major violations [Percent of the total number of individual passengers with major violations of customs and immigration laws and regulations that were apprehended based on statistical estimates of the total number of violations that came through our international airports]	43.5%
Land border apprehension rate for major violations. [Percent of the total number of vehicles travelers with major violations of customs and immigration laws and regulations that were apprehended based on statistical estimates of the total number of violations that came through the Points of Entry (POEs)]	37.5%
Percent of at-risk miles under strategic air surveillance.	95%
Percent of undocumented migrants who attempt to enter the U.S. via maritime routes that are interdicted [As estimated, based upon data obtained from the U.S. Coast Guard and U.S. Customs and Border Protection]	71.5%
Number of incursions into the U.S. exclusive economic zone (EEZ)	185
Percent of time that Coast Guard assets included in the Combatant Commander Operational Plans are ready at a Status of Resources and Training System (SORTS) rating of 2 or better.	100%
* The degree of effective control will be determined by the resources devoted to the task as developed in the Department's FY 2010–14 budget proposal and by funding provided by Congress.	

Figure 12.2 Goal 1 performance. (From One Team, One Mission, Securing the Homeland, 2008–2013.)



Figure 12.3 Bering Sea: the Coast Guard cutter Healy breaks ice around the Russian-flagged tanker vessel Renda 250 miles south of Nome, Alaska, January 6, 2012. (From U.S. Coast Guard (Photo by Petty Officer 1st Class Sara Francis.))

DHS as a whole could learn much from this key player in both emergency response and homeland defense roles (Figure 12.3).

At present, DHS seemingly continues down a path of agency building by looking for more fields of coverage and control. With a nation \$28 trillion in debt and counting, and a military complex now facing severe and significant cuts, little—including DHS's massive budget—will be spared the budgetary realities of the decade to come.⁸

Internet Exercise: Visit the U.S. Debt Clock to get some sense of how staggering our national debt has become at <http://www.usdebtclock.org>.

12.2 Growth without Reason

From its inception, DHS was running on a different clock than its governmental counterparts. Aside from its origination, it could change like a chameleon. Today's threat was tomorrow's agenda item, only lower on the list. DHS could consume, like a ravenous beast, most of its competing agencies, even those with a historically different approach. Nothing is all that surprising about bureaucracies growing, self-perpetuating, and feeding on mission to develop other parts of the bureaucratic puzzle. Yet this journey is neither a trek nor a run, but a propulsion that simply knows no bounds. FEMA's inclusion in DHS is an excellent illustration of this phenomenon. In FEMA, the natural disaster sets the tone—the hurricane, the earthquake, the fire, and so on. That is what FEMA was intended to direct its energies toward. Even so, FEMA would be subsumed into the DHS model. Some have wondered whether this tendency to simply swallow any event resembling a disaster has been good for DHS or FEMA. It is a question worth asking, and in the hubbub of growth and bureaucratic delirium, a pandemic of frenzy if there ever was one, one must stop and smell the roses. To grow and evolve is natural. To grow without much thought is mindless. Maybe FEMA's response to hurricane damage is not really the building blocks of DHS. Maybe earthquakes are flat out different and do not benefit from the DHS mentality. While not perfect, the generally positive signs in the planning in advance of and in response to Hurricane Sandy in the fall of 2012 indicate that FEMA may in fact be able to operate and function successfully within DHS. Certainly, the leadership, response, and rebuilding efforts in the wake of Sandy show remarkable improvement over such efforts during, and in the wake of,

Homeland Security

Hurricane Katrina. During recent disasters in the United States, whether flooding in Houston or North Carolina and fires in California to agricultural damage in the nation's Midwest, FEMA has largely performed above expectations. And FEMA's Strategic Plan says much of its own self-introspection and desire to fit its mission into a larger order. See Appendix E.⁹

As you read through the pages of this text, you have witnessed growth in both form and substance. You have witnessed the absorption of departments at a pace never seen before. You have gleaned that the term *infrastructure* means more than brick and mortar—that the FDA has a homeland plan just as the National Monuments Agency does. Everyone has a plan. Everyone combats terrorism. Page by page you have read about new plans, new stratagems, new policies, new mergers, and realignments. You can get dizzy reading about these changes. And one other thing—you can be sure that what is here likely will be different in a short time. I contend that more is not always more. Sometimes more is less. Fewer results, less efficiency, less coordination. Is it possible to take on too many agencies, too much responsibility, and thus lose the focus of what is truly important or necessary?

As an example, does the hiring of 60,000 new border agents—throwing sheer numbers at the problem—automatically guarantee a more secure border? Or is the border today any safer or more reassuring than 3 years ago? There is no definitive answer to such questions and while there has been progress in some areas, results are dubious at best in others.

Revisiting policy and enforcing current laws on the books would take care of many of the issues. We build fences, at least partial ones, to keep people out, but illegal immigration is still a consistent problem. While border security is necessary, a more holistic policy solution would include (1) increased border security in conjunction with encouraging legitimate immigration and naturalization and (2) a more consistent policy on illegal immigrants within the country. Establishing a reliable, efficient process for those individuals and families who are in the country now and want to become U.S. citizens would help alleviate some of the strain on the system, set the proper tone, and provide a clear and consistent path to obtaining citizenship. Current considerations around taking in foreign refugees, including those from the Syrian or any other conflict, or whether the United States simply be a “refuge” for the poor, cause serious and impassioned debate. Much of the discussion surrounds the identification and vetting of individuals before taking them into our country. In addition, there is the overall perception of other countries to consider—about our willingness to help, or not, as a world power and leader in what is inarguably a human rights crisis. At present, it remains to be seen how all will play out, although there have been some improvements at the border especially because of nation-to-nation agreements.

Why do our agencies neglect, and fail to unearth, serious potential targets, while they continue to search the 9-year-old child's Minecraft backpack or the coat of an 80-year-old grandmother? These are just singular, but simple and reflective examples of a department that does things in ways that belie notions of efficiency and targeted focus. A DHS that operates as the agency does at present will not last into the next century. It will not be nimble enough to last. Even DHS knows this reality. In 2010, DHS announced a threefold mission concerning how it will unfold in the decade to come: first, it will need to consolidate duplicitous operations; second, it will need to streamline these bulky and cumbersome systems; and lastly, it will need to be open to the world. Talk of change is in the air, and whether the nature and sheer size of DHS can adapt remain unclear. DHS is well meaning when it relays the following:

We have taken significant steps to create a unified and integrated department that will enhance our performance by focusing on:

- Accountability
- Efficiency
- Transparency, and

- Leadership development (One Team, One Mission, Securing the Homeland, 2008–2013)

Its 2018, Strategic Plan continues this direction by adopting three Strategic Goals, namely:

- Build a Culture of Preparedness
- Ready the Nation for Catastrophic Disasters
- Reduce the Complexity of FEMA¹⁰

The future of homeland security can be prosperous and highly effective; it can help prevent attacks and thwart the terrorist who seeks to disrupt and destroy our way of life. Ultimately, it can provide levels of security and safety at costs more aligned with reality and the mission of government in general.

12.3 Curbing Expansionism in Mission

To have any chance at a prosperous future, DHS will have to simplify. There is too much under its roof, and much of what sits under its tent does not belong. DHS's new mission encompasses the following:

Three key concepts form the foundation of our national homeland security strategy designed to achieve this vision:

- Security
- Resilience
- Customs and Exchange

The Guiding Principles of the DHS are:

- Champion “Relentless Resilience” for All Threats and Hazards
- Reduce the Nation’s Risk to Homeland Security Dangers
- Promote Citizen Engagement and Strengthen and Expand Trusted Partnerships
- Uphold Privacy, Transparency, Civil Rights, and Civil Liberties
- Ensure Mission-Driven Management and Integration¹¹

The simplicity of the Guiding Principles and mission—a safer America through secure borders and the deterrence and prevention of terrorism—causes one to pause on the expansionist mentality that has occurred with the growth of DHS. The agencies in Table 12.1 became part of DHS in 2003. The table lays out the first expansionist event in the history of DHS.

Just for the sake of argument, does the merger and consolidation make sense in all cases? Can the Secret Service not carry out its mission without being tethered to DHS? What about the Energy Security and Assurance Program? Does DHS have the expertise to handle the subject matter? And the Plum Island Animal Disease Center—would it not make better sense to leave Plum Island with the Department of Agriculture? Does it seem likely that a terrorist event would occur with livestock? Noted already was the suitability of the FEMA merger. Why would hurricane response assist in DHS's mission? It is the author's view that DHS is struggling with its own identity, from its initial manifestation to its subsequent transformations. Instead of being attentive to its basic mission of security and counterterrorism, it has wandered into peripheral territory, only partially touching on questions of security. The net effect of this expansionism has been the dilution of other services and functions in government. Some departments are underfunded budget-wise and are adapting to missions that are tangential to their overall purpose.¹² For DHS to survive into the future, it may require shedding functions that stand far

Table 12.1 Departmental Movements in the History of DHS

Original Agency (Department)	Current Agency/Office
The U.S. Customs Service (Treasury)	U.S. Customs and Border Protection: Inspection, border, and ports of entry responsibilities U.S. Immigration and Customs Enforcement: customs law enforcement responsibilities
The Immigration and Naturalization Service (Justice)	U.S. Customs and Border Protection: Inspection functions and the U.S. Border Patrol U.S. Immigration and Customs Enforcement: Immigration law enforcement; detention and removal, intelligence, and investigation U.S. Citizenship and Immigration Services: Adjudications and benefits programs
The Federal Protective Service	U.S. Immigration and Customs Enforcement
TSA (Transportation)	TSA
Federal Law Enforcement Training Center (Treasury)	Federal Law Enforcement Training Center
Animal and Plant Health Inspection Service (part) (Agriculture)	U.S. Customs and Border Protection: Agricultural imports and entry inspections
Office for Domestic Preparedness (Justice)	Responsibilities distributed within FEMA
FEMA	FEMA
Strategic National Stockpile and the National Disaster Medical System (HHS)	Returned to HHS, July 2004
Nuclear Incident Response Team (Energy)	Responsibilities distributed within FEMA
Domestic Emergency Support Teams (Justice)	Responsibilities distributed within FEMA
National Domestic Preparedness Office (FBI)	Responsibilities distributed within FEMA
Chemical, Biological, Radiological, and Nuclear Countermeasures Programs (Energy)	Science and Technology Directorate
Environmental Measurements Laboratory (Energy)	Science and Technology Directorate
National Biodefense Defense Analysis Center (Defense)	Science and Technology Directorate
Plum Island Animal Disease Center (Agriculture)	Science and Technology Directorate
Federal Computer Incident Response Center (GSA)	US-CERT, Office of Cyber Security and Communications in the National Programs and Preparedness Directorate
National Communications System (Defense)	Office of Cyber Security and Communications in the National Programs and Preparedness Directorate

(Continued)

Table 12.1 (Continued) Departmental Movements in the History of DHS

Original Agency (Department)	Current Agency/Office
National Infrastructure Protection Center (FBI)	Dispersed throughout the department, including the Office of Operations Coordination and the Office of Infrastructure Protection
Energy Security and Assurance Program (Energy)	Integrated into the Office of Infrastructure Protection
U.S. Coast Guard	U.S. Coast Guard
U.S. Secret Service	U.S. Secret Service

afield from its ultimate end or purpose. William L. Waugh Jr. notes in “The Future of Homeland Security and Emergency Management”:

Mission problems were expected with the integration of non-terrorism programs into a department focused on the terrorist threat. FEMA, in particular, has responsibilities unrelated to dealing with terrorism, such as the National Flood Insurance Program and the National Earthquake Hazard Reduction Program. Other DHS components also have diverse non-terrorism responsibilities, not least of which are the U.S. Coast Guard’s responsibilities related to oil spills, boating safety, and air-sea rescue.¹³

It is a legitimate critique, for why does DHS involve itself in flood insurance, geospatial maps, and computer security breaches? Are these activities consistent with mission or causing stress internally and externally? To be sure, the financial stress alone, the budgetary demands of new obligations, has either drained historic budgets or added to tightness in existing budgets.

By 2005, departmental changes were being referred to as *structural adjustments*. Change continued its unabated pace with new recommendations for the department. New offices, directors, realignments, and mergers continued without reservation. For example, a new Director of Operations Coordination was implemented. The director’s primary function was to improve coordination and efficiency of operations. By this time, DHS was tackling so many functions that it was feeling the pressure and stress of nonaligned functions. Why else would DHS need a Director of Operations Coordination?

In general, DHS continues to realign itself and is trying to serve many masters. For the future health of the agency, DHS may need to adhere to a different model that sticks to the fundamentals of what the department can and should do. To that end, what the future holds remains to be seen.

12.4 The Merits of Decentralization

While DHS touts the value of the decentralized model in much of its literature, it has erected centralized superstructures of operations. DHS is about as centralized a department as it gets. It is overly large and overly bureaucratic on a number of levels.

In August 2011, the traditionally conservative think tank the Heritage Foundation urged DHS to engage in the sort of decentralizing self-assessment that would cause culture shock. In short, get smaller by spinning off the responsibilities or return them to the place from which they were originally grabbed. By 2015, critics of DHS had become a far more common force in the appropriations process to continually fund it, and in the intellectual and think tank constituencies that critique its operations.¹⁴ Give back to the states and localities, that know

Homeland Security

their populations, and the local task of homeland defense. One must coordinate, but not at the expense of statewide and local visions. Their recommendations:

- Establishing a framework for empowering state and local authorities to meet their responsibilities for disaster response and domestic counterterrorism operations, particularly for ensuring state and local input into national policies and promoting intelligence-led policing.
- Adopting a fair, honest, and realistic approach to immigration enforcement that recognizes state and local authorities as responsible partners and abjures an “amnesty first” strategy, which would simply encourage more illegal border crossings and unlawful presence. Sensible and functional border security, immigration, and workplace laws are vital to focusing scarce resources on the pressing security threat posed by transnational criminal cartels based in Mexico.
- Overhauling the process for declaring federal disasters and dispensing homeland security grants. Current policies and programs waste resources and do not promote resiliency or preparedness.
- Maintaining the use of key counterterrorism tools, such as those authorized under the USA PATRIOT Act, and establishing a national domestic counterterrorism and intelligence framework that clearly articulates how intelligence operations at all levels should function to combat terrorism.
- Rethinking the Transportation Security Administration (TSA) and restructuring its mission from providing airport security to making aviation security policy and regulations and devolving screening responsibility to the airport level under supervision of a federal security director.¹⁵

In 2018, a similar critique was posited by the Heritage Foundation by asking DHS to “reinvent” itself.¹⁶ While any of these points can be, and have been, debated from multiple angles, this list does identify some of the key issues at the heart of homeland security and the future of DHS. Consensus opinion among many in and around government circles confirms that to change tack and move in a new direction will require a major cultural shift in how the respective agencies within DHS see and appreciate the responsibilities of homeland security. This will not happen overnight.

Despite this, there are positive signs of regional, state, and local cooperation. Advisory councils and committees exist to foster local influence. Partnerships abound with the federal DHS and states and localities. Although these are steps in the right direction, it is clear that federalism reigns supreme in the affairs of homeland security. In grants, in policymaking, in budgetary allotments, in federal appointments to staff positions, the federal system dominates the states and localities. This domination diminishes the role of local input and control in matters of homeland security.

To that end, Samuel Clovis Jr. proposes the following characteristics of collaborative federalism for homeland security:

- Homeland security is a national issue requiring national solutions. As such, the role of Congress and its executive agent DHS is that of facilitation and leadership, providing guidelines, milestones, and enough funding to make a difference.
- State and local governments have maximum flexibility in implementing homeland security programs to gain greater efficiency and better situational awareness.¹⁷

Collaboration signifies meaningful input and participation rather than a sometimes-formulaic reaction to posted policy and funding mechanisms. Instead of implementing one-size-fits-all states and localities, DHS might be better served looking to the localities for their needs assessment and turning over more tasks and functions to localities.

12.5 The Rise of Technology

For too long, both prior to joining DHS and in their current structure, the many functions of homeland security have been performed manually by people, often at extraordinary cost. Covered in depth throughout this text were the more than 100,000 employees in TSA and Border Patrol. To have any future, DHS will have to operate with leaner staffing and financial budgets. It cannot survive long term with high payrolls necessitated by huge staffing, nor should some of the rote functions of TSA employees be reserved for personnel. It appears that machines can do a comparable job, and we may be on our way to seeing more and more reliability in technologies to help security functions. DHS already knows that science and technology will lead the way in any future for DHS. Just a few examples of current initiatives are shown in Figure 12.4.¹⁸

DHS Science and Technology Directorate

S&T Apex—An Overview of What an Apex is and How it Works

What are Apex Programs?

Apex Programs represent a change in the way the Science and Technology Directorate (S&T) manages research and development (R&D) programs and projects.

A collection of S&T projects, Apex Programs represent one or more paths toward achieving an increased or improved capability for the Homeland Security Enterprise (HSE). Resulting from a visionary goals, an S&T strategic priority, or an external stakeholder's operational need, Apex Programs take the next steps towards implementing solutions to improve the security and resilience of our nation.

The following Apex programs look strategically at the nation's security and address future challenges while continuing to support today's operational needs.

Air Entry/Exit Re-Engineering (AEER)

The AEER program was developed in partnership with U.S. Customs and Border Protection, to efficiently screen travelers entering the United States and to confirm the departure of non-U.S. citizens. AEER determines how to use new technologies and processes to expedite screening by evaluating current commercial biometric technologies to support air entry and emerging exit applications.

Border Situational Awareness (BSA)

The BSA program will enable the HSE to achieve increased border situational awareness. The goal of the Apex BSA program is to improve border situational awareness by establishing an enterprise capability to 1) access more data sources, 2) make available decision support tools, and 3) share that actionable information and intelligence with partner law enforcement agencies.

Real-Time Biothreat Awareness

The Real-time Biothreat Awareness program aims to provide timely information to multiple authorities, enabling a collaborative and effective response that ultimately minimizes the impacts of a biological incident. Through this program, S&T will help authorities better prepare for incidents in which biological material is released.

Relational, Adaptive Processing of Information and Display (RAPID)

The RAPID program will save lives, reduce property losses, and enhance community resilience to disruptive events such as floods. With support from S&T, the Federal Emergency Management Agency will be able to 1) leverage existing data sources, 2) enhance collaboration and coordination, 3) identify indicators of community resilience, 4) empower communities with a decision support tool, and 5) enable faster speed-to-decision in the operational theater.

Next Generation Cyber Infrastructure

The Next Generation Cyber Infrastructure program will address the challenges facing our nation's critical infrastructure sectors, enabling infrastructure to operate effectively, even in the face of sophisticated, targeted cyberattacks. The program seeks to provide technologies and tools to protect critical systems and networks.

Aviation Checkpoint Screening at Speed (ACSAS)

The Aviation Checkpoint Screening at Speed program seeks to create an almost-invisible checkpoint by integrating imaging, trace detection, X-ray technologies, and software systems. S&T is working with the Transportation Security Administration, Department of Energy national laboratories, universities, and industry on this program. The goal is to reduce invasiveness and inconvenience to passengers while increasing capability to respond to evolving threats.

Next Generation First Responder (NGFR)

The NGFR program seeks to develop a scalable and modular ensemble that includes an enhanced duty uniform, personal protective equipment, wearable computing and sensing technology, and robust voice and data communication networks. NGFR will harness the best existing and emerging technologies and integrate them in a well-defined and standards-based open architecture.



Homeland Security

Science and Technology

To learn more about Apex Programs visit <http://www.dhs.gov/science-and-technology/apex-programs>,
contact: apexescsecretariat@hq.dhs.gov

2015-07-

Figure 12.4 DHS Science & Technology Directorate Apex programs.

Homeland Security

DHS's reliance on outside authority and analysis is one of its greatest recent accomplishments. DHS has aggressively developed partnerships with universities and colleges, as well as private associations, nonprofits, think tanks, and research centers, including its many designated "Centers for Excellence." Such partnerships include

- Center for Borders, Trade, and Immigration Research (CBTIR), led by the University of Houston, develops technology-based tools, techniques, and educational programs for border management, immigration, trade facilitation, and targeting and enforcement of transnational borders.
- Coastal Resilience Center of Excellence (CRC), led by the University of North Carolina at Chapel Hill, conducts research and education to enhance the Nation's ability to safeguard people, infrastructure, and economies from catastrophic coastal natural disasters such as floods and hurricanes.
- Critical Infrastructure Resilience Institute (CIRI), led by the University of Illinois at Urbana-Champaign, conducts research and education to enhance the resilience of the Nation's critical infrastructure and its owners and operators.
- Arctic Domain Awareness Center of Excellence (ADAC), led by the University of Alaska Anchorage, develops and transitions technology solutions, innovative products, and educational programs to improve situational awareness and crisis response capabilities related to emerging maritime challenges posed by the dynamic Arctic environment.
- Center for Visualization and Data Analytics (CVADA), co-led by Purdue University (visualization sciences—VACCINE) and Rutgers University (data sciences—CCICADA), creates the scientific basis and enduring technologies needed to analyze large quantities of information to detect security threats to the nation.
- Center of Excellence for Awareness and Localization of Explosives-Related Threats (ALERT), led by Northeastern University, develops new means and methods to protect the nation from explosives-related threats.
- Center of Excellence for Zoonotic and Animal Disease Defense (ZADD), co-led by Texas A&M University and Kansas State University, protects the nation's agriculture and public health sectors against high-consequence foreign animal, emerging and zoonotic disease threats.
- Food Protection and Defense Institute (FPDI), led by the University of Minnesota, defends the safety and security of the food system by conducting research to protect vulnerabilities in the food supply chain. FPDI was formerly named the National Center for Food Protection and Defense (NCFPD).
- Maritime Security Center of Excellence (MSC), led by Stevens Institute of Technology, enhances Maritime Domain Awareness and develops strategies to support Marine Transportation System resilience and educational programs for current and aspiring homeland security practitioners.
- National Center for Risk and Economic Analysis of Terrorism Events (CREATE), led by the University of Southern California, develops advanced tools to evaluate the risks, costs, and consequences of terrorism.
- National Consortium for the Study of Terrorism and Responses to Terrorism (START), led by the University of Maryland, provides policy makers and practitioners with empirically grounded findings on the human elements of the terrorist threat and informs decisions on how to disrupt terrorists and terrorist groups.

- Center for Maritime, Island and Remote and Extreme Environment Security (MIREES), co-led by the University of Hawaii and Stevens Institute of Technology, focuses on developing robust research and education programs addressing maritime domain awareness to safeguard populations and properties in geographical areas that present significant security challenges.
- Center for Advancing Microbial Risk Assessment (CAMRA), co-led by Michigan State University and Drexel University and established jointly with the U.S. Environmental Protection Agency, fills critical gaps in risk assessments for mitigating microbial hazards.
- Coastal Hazards Center of Excellence (CHC), co-led by the University of North Carolina at Chapel Hill and Jackson State University, performs research and develops education programs to enhance the nation's ability to safeguard populations, properties and economies from catastrophic natural disasters.
- National Center for Border Security and Immigration (NCBSI), co-led by the University of Arizona and the University of Texas at El Paso, develops novel technologies, tools, and advanced methods to balance immigration and commerce with effective border security.
- National Center for the Study of Preparedness and Catastrophic Event Response (PACER), led by Johns Hopkins University, optimizes the nation's medical and public health preparedness, mitigation, and recovery strategies in the event of a high-consequence natural or man-made disaster.
- National Transportation Security Center of Excellence (NTSCOE) was established in accordance with H.R.1, implementing the Recommendations of the 9/11 Commission Act of 2007, in August 2007. NTSCOE is a seven-institution consortium focused on developing new technologies, tools, and advanced methods to defend, protect, and increase the resilience of the nation's multimodal transportation infrastructure.¹⁹

DHS is currently devising new APEX programs that apply technological solutions to homeland dilemmas. Of particular interest are the innovative solution in travel and screening. Here are a few examples of the new programs.

- The Apex Air Entry/Exit Re-engineering (AEER) program, developed in partnership with U.S. Customs and Border Protection (CBP), seeks ways to increase CBP's capacity to screen travelers entering the United States and to confirm the departure of non-U.S. citizens from U.S. airports. AEER determines how to use new technologies and processes to expedite screening by evaluating current commercial biometric technologies to support air entry and emerging exit applications. For more information on the AEER program, contact aer@hq.dhs.gov.
- The Apex Border Situational Awareness (BSA) program will enable the Homeland Security Enterprise to achieve increased border situational awareness, leading to increased border incursion detection, interdictions, and deterrence. CBP and partner law enforcement agencies (federal, state, local, tribal, international) need improved situational awareness to more effectively and efficiently deploy resources to the areas of highest risk, especially along the land border between the ports of entry on the U.S. southwest border. The goal of the Apex BSA program is to improve border situational awareness by establishing an enterprise capability to (1) access more data sources, (2) make available decision support tools to translate the available data into actionable information and intelligence, and (3) share that actionable information and intelligence with partner law enforcement agencies.

Homeland Security

- The Apex Real-Time Biothreat Awareness program aims to provide timely information to multiple authorities, enabling a collaborative, confident, and effective response that ultimately minimizes the impacts of a biological incident. DHS envisions a biosurveillance system that integrates and analyzes data from multiple sources and provides real-time, actionable information. Through this program, S&T will help authorities better prepare for incidents in which biological material is released. Authorities will be able to quickly gain situational awareness about the potential biological threat, the exposed population, and the likelihood of infection to provide responders and decision makers with the data needed to make informed, confident decisions that will save lives and money and restore normal operations quickly.
- The Apex Next Generation Cyber Infrastructure program addresses the challenges facing our nation's critical infrastructure sectors, enabling infrastructure to operate effectively, even in the face of sophisticated, targeted cyberattacks. The program seeks to provide technologies and tools to protect critical systems and networks. This includes the ability to (1) detect the presence of a cyberthreat without relying on a known cyber signature, (2) understand how the threat impacts operations, and (3) neutralize the threat in a manner that does not impact operations. This project will initially work in partnership with the financial sector but will be expanded later.²⁰

In the coming years, technology will replace the human person in carrying out the mission of DHS in many cases, hopefully for the better. While controversial in many circles, many planes and helicopter applications are poised to be replaced with drones for use in border security, surveillance, law enforcement, and search and rescue operations, although drones have been challenged on both functional and constitutional fronts (Figure 12.5).²¹

TSA employees, who presently search bags and laptops, will continue to be aided by new and emerging technologies (Figure 12.6).

DHS and its Science and Technology Directorate know keenly where the winds are blowing—to science and the role of technology securing the country (Figure 12.7).²²

This trend will continue into the long-term future. With new products and designs to track cargo, to sniff out explosives, to detect biological agents, and to prevent IED explosions, the role of technology will only increase in the years to come.

Other areas in need of innovation and creative upgrade are surveillance practice, sensor capacity, robotics in hazardous situations, and new methods and protocols in all aspects of information technology. On top of these challenges, the virtual reality all of us find ourselves



Figure 12.5 Air force drone.

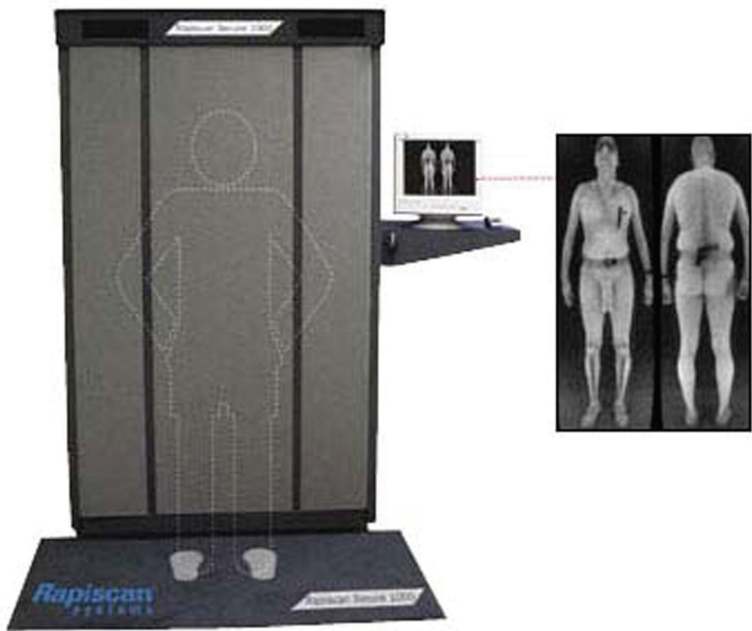


Figure 12.6 Millimeter wave.

BUDGET REQUEST
Dollars in Thousands

	2019 Enacted		2020 Enacted		2021 President's Budget		2020 - 2021 Total Changes	
	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
Operations and Support	473	\$308,520	499	\$314,864	456	\$284,789	(43)	(\$30,075)
Procurement, Construction and Improvement	-	-	-	-	-	\$18,927	-	\$18,927
Research and Development	-	\$511,265	-	\$422,411	-	\$340,013	-	(\$82,398)
Net Discretionary	473	\$819,785	499	\$737,275	456	\$643,729	(43)	(\$93,546)
Gross Discretionary	473	\$819,785	499	\$737,275	456	\$643,729	(43)	(\$93,546)
Total Budget Authority	473	\$819,785	499	\$737,275	456	\$643,729	(43)	(\$93,546)
Less: Rescissions to Prior Year Balances	-	\$533	-	\$273	-	-	-	(\$273)
Total	473	\$819,252	499	\$737,002	456	\$643,729	(43)	(\$93,273)

*FTE reported in this table may differ from MAX A-11 due to adjusted Budget Year (BY) estimates.

Figure 12.7 Though future funding and budgets may be tight, there needs to be a commitment to long-term technology that functional serves and advances Homeland Security needs.

entangled with—in commerce and social media, in finance and government benefits, in credit cards and check deposits—is the brave new world of cybersecurity.²³

Reality and the virtual world are now natural, interconnected handmaidens rather than separate entities, for it is crucial that we learn how to fight in both theaters of war. As a result, the DHS of the future will rely on technology in a much more substantial way than today.

12.6 The Need for a New Way of Thinking: Jump Out of the Box

Much of what has and continues to take place in homeland security has taken place with limited to little objection. It is hard to argue that terrorism is a growing global and domestic threat and that it makes sense to take efforts to ensure the country's safety and security. However, it would be wise to take a step back, assess, and consider what we are doing and what needs to be done by way of homeland security. I mean this in three different senses.

First, why do we do what we do in so mechanically and repetitively? Is the threat as real and substantial as described? If the threats were as real and meaningful as the experts indicate, would these events not occur with greater regularity? Is it really necessary to check passengers in airports as presently done? Is there some proof, if we chose not to frisk and search people, that terrorism would rise without resistance? More people die in suicide and car crashes each year, and government appears unable to fully thwart these tragedies. Why are we so sure of our methods? Why is a government response the best preventive tool? Do more procedures automatically translate to greater security? Today there has yet to be another aircraft terrorism event at the scope and size of 9/11, though not for lack of trying (refer to the Christmas Day bomber mentioned in Chapter 2), yet we continue our TSA regimen without hesitation. Yet this is not to say that history cannot repeat itself.

Currently under investigation is whether the Russian airplane en route from Egypt was the victim of terror bomb plant. ISIS has taken credit for the destruction. Russia is claiming a bomb brought down the Metrojet airbus, but the Egyptian government is still inconclusive on the matter.²⁴ Or one might interpret events and circumstances, or the lack thereof, as the natural result of a diligent and enlightened security program. Others might argue sheer coincidence or luck, or that the terrorist has altered their methodology. Whatever the answer might be, it is sound policy to ask whether the TSA investment, as it currently stands, is justified? Or have we ever considered that our fears are disproportionate to the potential risk or harm? Why do we assume these fears are properly correlated?

Benjamin Freidman's *Managing Fear: The Politics of Homeland Security*²⁵ forces this sort of examination—begging whether fear can be justified in its present form. He is particularly piercing when he engages in the threat of bioterrorism.

Eight years later and counting, with plenty of conventional terrorism abroad and almost none in the United States, evidence is mounting that these trends are overstated or wrong—that September 11 was more an aberration than a harbinger of an age of deadlier terrorism. Terrorism using biological or nuclear weapons should still worry us, but the common claim that these sorts of attacks are virtually inevitable is an overstatement.²⁶

Freidman goes on to further argue that our fears may be “inflated” and, given this reality, it is just the place for a bureaucrat to find a comfy nest.²⁷

The argument here is to think beyond the status quo and the normative. Thinking outside any box is not an easy task, and thinking outside a governmental box is almost an impossibility. Yet, this is what must happen in order for DHS to thrive into the next century. It cannot use law enforcement techniques suitable for the twentieth century when, in some cases, technology can substitute. Homeland professionals of the future should not accept the status quo and need to look beyond the holiday and the personal day. Leap out of the box and do things differently than the traditional way of doing task and function. A few examples of this thinking might be to

- Target terrorists through behavioral profiling
- Have random rather than mandatory checkpoints at air and transportation facilities
- Allow frequent fliers to skip security systems; this has been done for registered fliers on an increasing basis
- Allow local police authorities to assume some homeland functions

- Insist on a grant program that is not universally applied but targeted to localities and their needs
- Disburse budgetary allotments at the local level
- Return non-DHS functions to previous agencies
- Halt the onerous license requirements for American citizens
- Decentralize more DHS operations to the states and localities

These are representative suggestions for how DHS and its staff might think outside the usual constraints.

In general, the future of DHS largely depends on the demand due to circumstance, incident, and event, and whether the functions of response remain local or national responsibilities. Regardless, we know with certainty that terrorism is not going away, and, at a minimum, this assures a long-term place and need for the Department of Homeland Security.

Notes

- 1 DHS, Statement by secretary Jeh C. Johnson on the 2015 federal employee viewpoint survey results (September 28, 2015), <http://www.dhs.gov/news/2015/09/28/statement-secretary-jeh-c-johnson-2015-federal-employee-viewpoint-survey-results> (accessed August 22, 2020).
- 2 W. V. Pelfrey, Sr. and W. V. Pelfrey, Jr., Sensemaking in a nascent field: A conceptual framework for understanding the emerging discipline of homeland security, *The Homeland Security Review*, 4 (2010): 161.
- 3 FBI, *A Study of Active Shooter Incidents in the United States between 2000 and 2013* (Washington, DC: Texas State University and FBI, 2013), <https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2018-041019.pdf/view> (accessed August 22, 2020).
- 4 FBI, Quick Look: 277 Active Shooter Incidents in the United States from 2000 to 2018, <https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics> (accessed August 22, 2020).
- 5 FEMA, *FEMA Strategic Plan: Fiscal Years 2011–2014*, FEMA P-806 (Washington, DC: DHS, February, 2011), http://www.fema.gov/pdf/about/strategic_plan11.pdf (accessed August 22, 2020).
- 6 DHS, *One Team, One Mission, Securing Our Homeland*.
- 7 U.S. Coast Guard, *Posture Statement 2021 Budget Overview 7* (Washington, DC: USCG, February 2011), <https://www.uscg.mil/portals/0/bib/BIB-booklet-FINAL-v3-web.pdf> (accessed August 22, 2020).
- 8 E. Beidel, Homeland security market “vibrant” despite budgetary concerns, *National Defense*, September 2011, 34. For a full view of research and development funds for DHS, see: Congressional Research Service, *Federal Research and Development Funding: FY2011* (Washington, DC: Library of Congress, March 25, 2011).
- 9 FEMA, Strategic Plan, Appendix A: Performance Measures (2018), <https://www.fema.gov/media-library-data/1539201906346-182cf937905ffcca02512f489f51b791/appendixa.pdf> (accessed August 22, 2020).
- 10 Ibid.
- 11 See US Dept of Homeland Security, Guiding Principles webpage, <https://www.dhs.gov/guiding-principles> (accessed August 22, 2020).
- 12 D. M. West, A vision for homeland security in the year 2025, Governance Studies at Brookings, June 26, 2012, http://www.insidepolitics.org/brookingsreports/homeland_security.pdf (accessed August 22, 2020).
- 13 W. L. Waugh, Jr., *Future of Homeland Security and Emergency Management* (Emmitsburg, MD: Emergency Management Institute, 2011).
- 14 P. Fredrick and D. Inserra, An Opportunity for Real Reform at DHS, The Heritage Foundation, at March 9, 2018, <https://www.heritage.org/homeland-security/commentary/opportunity-real-reform-dhs> (accessed August 22, 2020).

Homeland Security

- 15 See M. Mayer, J. J. Carafano, and J. Zuckerman, Homeland security 4.0: Overcoming centralization, complacency, and politics, Heritage Foundation Special Report #97 (August 23, 2011), <http://www.heritage.org/research/reports/2011/08/homeland-security-4-0-overcoming-centralization-complacency-and-politics> (accessed August 22, 2020).
- 16 P. Fredrick and D. Inserra, An Opportunity for Real Reform at DHS, The Heritage Foundation, at March 9, 2018, <https://www.heritage.org/homeland-security/commentary/opportunity-real-reform-dhs> (accessed August 22, 2020).
- 17 S. H. Clovis, Jr., Federalism, homeland security and national preparedness: A case study in the development of public policy, *Homeland Security Affairs*, 2 (October 2006): 17.
- 18 SU Dept of Homeland Security Science and Technology Directorate, S&T Apex-An Overview of What an Apex is and How it Works, <https://www.dhs.gov/sites/default/files/publications/Apex%20Overview.pdf>
- 19 DHS, Science and technology: Centers of excellence, <http://www.dhs.gov/science-and-technology/centers-excellence> (accessed August 22, 2020).
- 20 US Dept of Homeland Security Science and Technology Directorate, Apex Programs webpage, <https://www.dhs.gov/science-and-technology/apex-programs> (accessed August 22, 2020).
- 21 M. Peck, DHS's border drones prove ineffective, *Federal Times*, January 13, 2015, <https://www.federaltimes.com/management/2015/01/07/dhs-s-border-drones-prove-ineffective/> (accessed August 22, 2020); D. Sarkar, CBP's \$260M investment in drone border security program shows little return, DHS IG tells panel, *Fierce Government*, July 16, 2015; DHS, Office of Inspector General, U.S. customs and border protection's unmanned aircraft system program does not achieve intended results or recognize all costs of operations, OIG-15-17, December 24, 2014, https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-17_Dec14.pdf (accessed August 22, 2020).
- 22 US Dept of Homeland Security, 2021 Budget in Brief, https://www.dhs.gov/sites/default/files/publications/fy_2021_dhs_bib_0.pdf (accessed August 22, 2020).
- 23 DHS, *Blueprint for a Secure Cyber Future* (Washington, DC: DHS, 2015), <http://www.dhs.gov/blueprint-secure-cyber-future> (accessed August 22, 2020); See also: Jane Hartman, 'The Future of Homeland Security: The Evolution of the Homeland Security Department's Roles and Missions': Jane Harman Testifies before the Senate Committee on Homeland Security and Governmental Affairs, The Wilson Center, July 12, 2012, <https://www.wilsoncenter.org/article/the-future-homeland-security-the-evolution-the-homeland-security-departments-roles-and> (accessed August 22, 2020).
- 24 A. Aboulenein and L. Noueihed, Islamic State says "Schweppes bomb" used to bring down Russian plane, *Reuters* U.S. Online Edition (November 19, 2015), <http://www.reuters.com/article/us-egypt-crash-islamicstate-photo-idUSKCN0T725Q20151119> (accessed August 22, 2020).
- 25 B. York, *Washington Examiner*, January 9, 2011, <https://texasinsider.org/articles/journalists-urged-caution-after-ft-hood-now-race-to-blame-palin-after-arizona-shootings> (accessed August 22, 2020).
- 26 B. H. Friedman, Managing fear: The politics of homeland security, *Political Science Quarterly*, 126 (2011): 77, 80. See also M. Leitenberg, Assessing the threat of bioterrorism, in B. H. Friedman, J. Harper, and C. A. Preble, editors, *Terrorizing Ourselves: Why Counterterrorism is Failing and How to Fix It* (Washington, DC: Cato Institute, 2010), 162–163.
- 27 Friedman, Managing fear, 83.

Appendix A

United States Department of Homeland Security: Homeland Security Advisory Council

AI.1 Official Designation

Homeland Security Advisory Council (HSAC)

AI.2 Authority

This charter establishes HSAC under the authority of Title 6 United States Code, Section 451. This discretionary committee is established in accordance with and operates under the provisions of the Federal Advisory Committee Act (FACA), Title 5 United States Code, Appendix.

AI.3 Objectives and Scope of Activities

HSAC shall provide organizationally independent, strategic, timely, specific, and actionable advice to the Secretary and senior leadership on matters related to homeland security. HSAC serves strictly as an advisory body with the purpose of providing advice upon the request of the Secretary. HSAC advice to the Secretary may encompass:

- A. *Strategy and policy*: Recommendations for the development of strategies and policies that will further the Department's ability to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, or other emergencies.
- B. *Leadership and coordination*: Recommendations for improving the Department's leadership and coordination, internally across the Department, externally across the Federal Government, and among state, local, tribal governments, first responders, the private and nonprofit sectors, academia, and research communities.
- C. *Management and implementation*: Recommendations for the development and implementation of specific programs or initiatives to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, or other emergencies.
- D. *Evaluation and feedback*: Recommendations for the efficiency and effectiveness of Department of Homeland Security (DHS) programs to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, or other emergencies.

AI.4 Descriptions of Duties

The duties of the HSAC are solely advisory in nature.

U.S. Homeland Security Advisory Council

AI.5 Official to Whom the Committee Reports

HSAC reports to the Secretary of Homeland Security.

AI.6 Agency Responsible for Providing Necessary Support

DHS is responsible for providing financial and administrative support to the HSAC. Within DHS, the Office of Partnership and Engagement provides this support.

AI.7 Estimated Cost, Compensation, and Staff Support

Estimated annual operating costs for the HSAC are \$800,000.00 which includes travel and per diem, and other administrative expenses, and three Full-Time Equivalent employees to support the Council.

AI.8 Designated Federal Officer

A full-time or permanent part-time employee of DHS shall be appointed by the Secretary as the HSAC Designated Federal Officer (DFO). The DFO or the Alternate DFO shall approve or convene HSAC meetings; approve meeting agendas; attend all committee, subcommittee, and task force meetings; adjourn any meeting when the DFO determines adjournment to be in the public interest; and chair meetings in the absence of the Chair or Vice Chair, or as directed by the Secretary.

AI.9 Estimated Number and Frequency of Meetings

Meetings of the HSAC may be held with the approval of the DFO; it is expected that the HSAC will meet as frequently as the Secretary desires. Committee meetings are open to the public unless a determination that the meeting should be closed is made by the appropriate DHS official in accordance with DHS policy and directives, and with Title 5, United States Code, subsection (c) of Section 552b.

AI.10 Duration

Continuing.

AI.11 Termination

This charter is in effect for 2 years from the date it is filed with Congress unless sooner terminated. The charter may be renewed at the end of this 2-year period in accordance with Section 14 of FACA.

AI.12 Member Composition

HSAC shall be composed of not more than 40 members who are appointed by, and serve at the pleasure of, the Secretary.

All members shall serve as Special Government Employees as defined in section 202(a) of Title 18 United States Code. Term length shall be up to 3 years and approximately one-third of the terms shall expire each year to promote membership continuity and currency of expertise. In the event the HSAC terminates, all appointments to the committee shall terminate.

In order for the Secretary to fully leverage broad-ranging experience and education, the HSAC must be professionally, technically, and culturally diverse. These members shall all be national leaders found within diverse and appropriate professions and communities nationwide. The membership shall be drawn from the following fields:

Police, fire, emergency medical services, and public works;

Public health;

State, local, and tribal officials;

National policy makers;

Experts in academia and the research community; and

Leaders from the private sector including, but not limited to, owners and operators of critical industries, resources, and infrastructure.

AI.13 Officers

The Secretary shall designate a Chair and a Vice-Chair from among the appointed members of HSAC. The Vice-Chair will act as Chair in the absence or incapacity of the Chair or in the event of a vacancy in the office of the Chair.

AI.14 Subcommittees

The Secretary may establish subcommittees, task forces, or working groups for any purpose consistent with this charter. In the event the subcommittee or HSAC terminates, all appointments to the subcommittee shall terminate. Subcommittees shall be composed of a number of HSAC and non-HSAC members to be determined by the DFO. The DFO, with the consultation of the HSAC Chair, shall designate a Chair and Vice Chair for each of the subcommittees from among the HSAC's members.

Subcommittees may not work independently of HSAC and must present their work to HSAC for full deliberation and discussion. Subcommittees have no authority to make decisions on behalf of the HSAC and may not report directly to the Federal Government or any other entity.

AI.15 Recordkeeping

The records of HSAC, formally and informally established subcommittees or other subgroups of the committee, shall be handled in accordance with General Records Schedule 6.2 or other approved agency records disposition schedule. These records shall be available for public inspection and copying, in accordance with the *Freedom of Information Act* (Title 5, United States Code, section 552).

U.S. Homeland Security Advisory Council

AI.16 Filing Date

March 4, 2019

Agency Approval Date

March 8, 2019

GSA Consultation Date

March 11, 2019 Date

Filed with Congress

Source: US Department of Homeland Security, Homeland Security Advisory Council, https://www.dhs.gov/sites/default/files/publications/19_0311_hsic-charter.pdf

Appendix B

NIMS Implementation Objectives for Federal Departments and Agencies

The National Incident Management System (NIMS) has been a key component of U.S. incident management efforts since its release in 2004. The goal is helping to prepare the nation for catastrophic disasters by enabling unity of effort among organizations from across the country during incidents, no matter the size, complexity, or duration. This nationwide unity of effort hinges on a shared understanding of what “NIMS implementation” entails among state, local, tribal, territorial, and Federal entities as well as the private sector, nongovernmental, and faith-based organizations.

Federal departments and agencies play an important role in ensuring effective NIMS implementation.

Not only do they implement NIMS themselves, they also ensure that the systems and processes are in place to communicate and support NIMS implementation at all jurisdictional levels.

Homeland Security Presidential Directive-5 (HSPD-5), Management of Domestic Incidents, requires all Federal departments and agencies to formally adopt and maintain NIMS and use it in their individual domestic incident management activities, supporting full and robust preparedness across the nation.

Since the release of HSPD-5, FEMA has engaged its Federal stakeholders to identify implementation objectives necessary to enhance incident management throughout Federal departments and agencies, including their subcomponent organizations.

FEMA previously revised the Federal NIMS Implementation Objectives in 2009. In this current update, we seek to ensure the objectives are consistent with the third edition of the NIMS, published in October 2017. The third edition of NIMS retains the concepts and principles from the 2008 and 2004 versions while reflecting changes to laws, policies, and best practices. Additionally, the third edition of NIMS provides additional information on the roles of off-scene incident personnel such as senior leaders and emergency operations center workers.

This version continues to incorporate Federal stakeholder input with the goal of providing better clarity and usefulness in implementing and applying NIMS. To this end, FEMA developed implementation indicators and metrics for each implementation objective.

The indicators are examples of characteristics that are frequently associated with Federal departments and agencies that have achieved the objective. They are not requirements, nor are the indicators intended as a checklist for achieving the objectives. The indicators are a tool to assist Federal departments and agencies in meeting the new Implementation Objectives.

Taken together, these objectives and their associated indicators and metrics provide guidance for Federal departments and agencies to clarify the types of activities to be undertaken when implementing NIMS. Doing so will help ensure a common, comprehensive, and interoperable approach to sharing resources, coordinating and managing incidents, and communicating information critical to the successful implementation of NIMS.

NIMS Implementation Objectives

All.1 General

Vision: Policies and processes are in place to support NIMS implementation

1. *Objective:* Formal adoption, maintenance, and updating of the National Incident Management System.

Indicator: A current authorizing authority that designates NIMS as the incident management system for the federal department/agency, including associated sub-agencies and departments.

2. *Objective:* Designate and maintain a single point of contact (POC) to serve as the principal coordinator for the implementation and ongoing maintenance of NIMS.

Indicator: Submission of name and POC information to FEMA for the current NIMS point of contact. This POC should be responsible for the overall coordination, continuing development, and/or evaluation of NIMS-related activities for their departments and agencies, including subcomponent organizations.

3. *Objective:* Develop and conduct periodic reviews (at least once a year) of a continuous NIMS implementation or improvement plan in alignment with current NIMS doctrine as issued by FEMA.

Indicator: Documentation clarifying department/agency-specific incident positions, roles, and procedures in alignment with NIMS. Guidance specifying how NIMS implementation is incorporated into each incident or exercise after-action review.

4. *Objective:* Ensure that preparedness grantees adopt NIMS throughout their jurisdiction or organization to prevent, protect against, mitigate, respond to, and recover from incidents.

Indicator: Grants monitoring program includes NIMS implementation as eligibility and assessment criteria. NIMS eligibility criteria align with the NIMS Implementation Objectives for Local, State, Tribal, and Territorial Jurisdictions.

5. *Objective:* Ensure that incident personnel receive pertinent NIMS training in alignment with the NIMS Training Program.

Indicator: Official training guidance that specifies:

- Which training course incident personnel must take;
- How long incident personnel have to complete the training after they join the department or agency; and
- Frequency of refresher training.

All.2 Resource Management

Vision: Consistent, interoperable identification, management, and sharing of resources

1. *Objective:* Identify and inventory deployable incident resources consistent with national NIMS resource typing definitions and job titles/position qualifications, available through the Resource Typing Library Tool (RTLTL).

Indicator: Up-to-date resource inventory (such as the Incident Resource Inventory System) that uses national resource-typing definitions for all shareable or deployable resources. Standard operating procedures specify how to identify requirements, order

and acquire, mobilize, track and report, demobilize, reimburse, and restock resources during incidents.

2. *Objective:* Participate in a program for the qualification, certification, and credentialing of incident personnel that aligns with the National Qualification System (NQS).

Indicator: Official guidance documents specify how incident personnel are qualified, certified, and credentialed consistently with NQS guidance. Use of OneResponder, or similar system, to track and maintain personnel Position Task Books.

3. *Objective:* Promotion of public, nongovernmental, and private sector use of cooperative agreements (e.g., Mutual Aid Agreements, Memorandums of Understanding/Agreement, Letters of Agreement, and Interagency Agreements) in alignment with NIMS.

Indicator: Use of multiorganizational plans, plans, funding mechanisms, training, exercises, and after-action reports to develop and evaluate mutual aid agreements, indicating consistent use of NIMS structures, principles, and procedures.

All.3 Command and Coordination

Vision: Integrated decision making and unity of effort among all incident personnel

1. *Objective:* Apply the Incident Command System (ICS) as the standard approach to the on-scene command, control, and coordination of incidents.

Indicator: Operational plans, policies, standard operating procedures, organizational structures, and training address the NIMS concepts and principles of accountability, span of control, incident action planning, mutual aid, unity of command and effort, and resource management.

2. *Objective:* Organize and manage EOCs and EOC teams consistent with pertinent NIMS guidance.

Indicator: Emergency Operations Plans (EOP), Standard Operating Procedures (SOP), organizational charts, or training program materials reflecting NIMS EOC guidance.

3. *Objective:* Use MAC Groups/Policy Groups as the policy-level body during incidents to support resource prioritization and allocation, and enable decision making among elected and appointed officials and those responsible for incident response and recovery activities.

Indicator: Exercise or real-world incident documentation or after-action reports indicating consistent use of NIMS principles, procedures, and structures. Standard operating procedures (SOPs) describe MAC Group processes for senior leadership within the department/agency.

4. *Objective:* Gather, verify, coordinate, and disseminate public information during an incident to include the establishment and/or coordination of Joint Information System (JIS) and Joint Information Centers (JIC).

Indicator: Exercise or real-world incident documentation or after-action reports indicating consistent use of JIS principles, procedures, and structures. Standard operating procedures and emergency operations plans that reflect NIMS guidance such as the NIMS Management Characteristics, ICS, MAC Groups, and JIS.

NIMS Implementation Objectives

All.4 Communications and Information Management

Vision: Information gets to who it needs to, when it needs to, and in a means they can understand

1. *Objective:* Apply plain language and clear text communication standards.

Indicator: SOPs, standard operating guidelines, and training program materials direct the use of plain language and clear text for incident communications.

2. *Objective:* Enable interoperable and secure communications within and across jurisdictions and organizations.

Indicator: Exercise and/or real-world incident documentation and/or after-action reports indicate that:

- Communications and information systems are reliable and scalable, and can function in any type of incident;
- Communications systems are resilient and redundant;
- Incident data, networks, and systems are appropriately protected and secure;
- Appropriate communication guidance is incorporated into EOPs and supporting plans and annexes; and
- Incident communications personnel have experience establishing and supporting interoperable communications.

3. *Objective:* Develop, maintain, and implement procedures for data collection, analysis, and dissemination to meet organizational needs for situational awareness.

Indicator: Exercise or real-world incident documentation indicate that incident personnel are collecting, analyzing, and disseminating situational awareness effectively and consistently with NIMS guidance.

- Data collection, analysis, and dissemination plans and SOPs align with NIMS guidance on information management and NIMS command and coordination structures.

Source: FEMA Fact Sheet. https://www.fema.gov/media-library-data/1588865410538-7831de04c1f1f1dc9e2cb09a670b6825/Federal_NIMS_IO_05042020.pdf

Appendix C

Sanctuary Cities List¹

States

California
Colorado
Connecticut
Illinois
Massachusetts
New Jersey
New Mexico
New York
Oregon
Vermont
Washington

Cities and Counties

California

Alameda County
Berkley
Contra Costa County
Fremont, CA
Los Angeles County
Los Angeles
Monterey County
Napa County
Oakland
Riverside County
Sacramento County
San Bernardino County
San Diego County
San Francisco County/City
San Mateo County
Santa Ana
Santa Clara County
Santa Cruz County

Sanctuary Cities List

Sonoma County

Watsonville

Colorado

Arapahoe County

Aurora

Boulder County

Denver County/City

Garfield County

Grand County

Jefferson County

Larimer County

Mesa County

Pitkin County

Pueblo County

Routt County

San Miguel County

Weld County

Connecticut

East Haven

Hartford

Florida

Alachua County

Georgia

Clayton County

DeKalb County

Iowa

Benton County

Cass County

Fremont County

Greene County

Ida County

Iowa City

Jefferson County
Johnson County
Marion County
Monona County
Montgomery County
Pottawattamie County

Illinois

Chicago
Cook County

Kansas

Butler County
Harvey County

Louisiana

New Orleans

Massachusetts

Amherst
Boston
Cambridge
Concord
Lawrence
Newton
NorthamptonSomerville

Maryland

Baltimore
Montgomery County
Prince George's County

Michigan

Ingham County
Kalamazoo County
Kent County
Lansing
Wayne County

Sanctuary Cities List

Minnesota

Hennepin County

Mississippi

Jackson

Nebraska

Hall County

Sarpy County

New Jersey

Newark

New Mexico

Bernalillo County

San Miguel

Nevada

Washoe County

New York

Albany

Franklin County

Ithaca

Nassau County

New York City

Onondaga County

St. Lawrence County

Westchester County

North Carolina

Buncombe County

Durham County

Forsyth County

Mecklenburg County

Orange County

Wake County

Ohio

Franklin County

Oregon

Baker County

Clackamas County

Clatsop County

Coos County

Crook County

Curry County

Deschutes County

Douglas County

Eugene

Gilliam County

Grant County

Hood River County

Jackson County

Jefferson County

Josephine County

Lane County

Lincoln County

Linn County

Malheur County

Marion County

Multnomah County

Polk County

Sherman County

Springfield

Tillamook County

Umatilla County

Union County

Wallowa County

Wasco County

Washington County

Wheeler County

Yamhill County

Sanctuary Cities List

Pennsylvania

Bradford County
Bucks County
Butler County
Chester County
Clarion County
Dauphin County
Delaware County
Franklin County
Lehigh County
Lycoming County
Montgomery County
Montour County
Perry County
Philadelphia
Pike County
Westmoreland County

Rhode Island

Providence

Virginia

Alexandria
Arlington County
Chesterfield County
Fairfax County

Vermont

Burlington
Montpelier
Winooski

Washington

Chelan County
Clallam County
Clark County
Cowlitz County

Franklin County
Jefferson County
King County
Kitsap County
Pierce County
San Juan County
Skagit County
Snohomish County
Spokane County
Seattle
Thurston County
Walla Walla County
Wallowa County
Marysville
Whatcom County
Yakima County

Note

- 1 Center for Immigration Studies, at <https://cis.org/Map-Sanctuary-Cities-Counties-and-States>.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Appendix D

Incident Notification and Reporting Form



INSTRUCTIONS

INCIDENT NOTIFICATION AND REPORTING APHIS/CDC FORM 3 (THEFT/LOSS/RELEASE)

FORM APPROVED
OMB NO. 0579-0213
OMB NO. 0920-0576
EXP DATE: 10/31/2020

Answer all items completely and type or print in ink. Detailed instructions are available at <http://www.selectagents.gov/form3.html>. This report must be signed and submitted to either APHIS or CDC:

Animal and Plant Health Inspection Service
Agriculture Select Agent Services
4700 River Road Unit 2, Mailstop 22, Cubicle 1A07
Riverdale, MD 20737
FAX: (301) 734-3652
Email: AgSAS@aphis.usda.gov

Centers for Disease Control and Prevention
Division of Select Agents and Toxins
1600 Clifton Road NE, Mailstop A-46
Atlanta, GA 30329
FAX: (404) 471-8375
Email: form3@cdc.gov

Accession Number:

(For Program Use ONLY)

Submit completed form only once by either email, fax, or mail

SECTION A - ENTITY INFORMATION			
1. Name of Entity:		2. Entity Registration/ NRE Number (if applicable):	
3. Physical Address (NOT a post office box):		4. City:	5. State: 6. Zip Code:
7. Name of Responsible Official or Laboratory Supervisor:		8. Name of Principal Investigator:	
9. Telephone Number:	10. Fax Number:	11. Email address:	
SECTION B - INCIDENT INFORMATION			
1. Date and Time of Incident: MM/DD/YY	2. Date of Immediate Notification: MM/DD/YY	3. Type of Immediate Notification : ☐ Email ☐ Fax ☐ Telephone ☐ eFSAP	4. Location of Incident (bldg., room, equipment, etc.):
5. Name of Select Agent or Toxin:		6. Strain designation of Select Agent or Toxin:	7. Quantity (Unit (vial, plates, etc.):

☐ Additional Select Agents or Toxins listed in attached document

Incident Notification and Reporting Form

8. Type of Incident: ☐ Theft (After completing Section B. Go to Section C) ☐ Loss (After completing Section B. Go to Section D) ☐ Release/ Potential Exposure (After completing Section B. Go to Section E) Note: Please complete Appendix A, event timeline, to provide details on the theft/loss/release incident.	9. Severity of the incident: ☐ None ☐ Negligible ☐ Low ☐ Moderate ☐ High	10. What Biosafety Level did the incident occur? <table style="width: 100%; border: none;"> <tr> <td>☐ ABSL2</td> <td>☐ NIHBL2</td> </tr> <tr> <td>☐ ABSL3</td> <td>☐ NIHBL3</td> </tr> <tr> <td>☐ ABSL4</td> <td>☐ NIHBL4</td> </tr> <tr> <td>☐ ACL2</td> <td>☐ NIHBL2N</td> </tr> <tr> <td>☐ ACL3</td> <td>☐ NIHBL3N</td> </tr> <tr> <td>☐ ACL4</td> <td>☐ NIHBL4N</td> </tr> <tr> <td>☐ BSL2</td> <td>☐ NIHBL2-LS</td> </tr> <tr> <td>☐ BSL3</td> <td>☐ NIHBL3-LS</td> </tr> <tr> <td>☐ BSL4</td> <td>☐ NIHBL4-LS</td> </tr> <tr> <td>☐ BSL3 Ag</td> <td>☐ PPQ Agent</td> </tr> </table>	☐ ABSL2	☐ NIHBL2	☐ ABSL3	☐ NIHBL3	☐ ABSL4	☐ NIHBL4	☐ ACL2	☐ NIHBL2N	☐ ACL3	☐ NIHBL3N	☐ ACL4	☐ NIHBL4N	☐ BSL2	☐ NIHBL2-LS	☐ BSL3	☐ NIHBL3-LS	☐ BSL4	☐ NIHBL4-LS	☐ BSL3 Ag	☐ PPQ Agent
☐ ABSL2	☐ NIHBL2																					
☐ ABSL3	☐ NIHBL3																					
☐ ABSL4	☐ NIHBL4																					
☐ ACL2	☐ NIHBL2N																					
☐ ACL3	☐ NIHBL3N																					
☐ ACL4	☐ NIHBL4N																					
☐ BSL2	☐ NIHBL2-LS																					
☐ BSL3	☐ NIHBL3-LS																					
☐ BSL4	☐ NIHBL4-LS																					
☐ BSL3 Ag	☐ PPQ Agent																					
11. Is this incident associated with an APHIS/CDC Form 2 (Transfer): ☐ Yes (Fill out Appendix B, if incident occurred during transfer.) ☐ No APHIS/CDC Form 2 transfer #: _____	12. Is this incident associated with an APHIS/CDC Form 4 (Identification): ☐ Yes ☐ No APHIS/CDC Form 4 clinical ID#: _____																					

SECTION C - REPORT OF THEFT

1. Type of Theft: ☐ Forced Entry ☐ Insider/Insider-assisted access ☐ Unauthorized access	2. Has Local Law Enforcement been Notified: (If yes, complete sections C3-C5) ☐ Yes ☐ No	3. Local Law Enforcement Agency:
4. Local Law Enforcement Agent Name: First MI Last		5. Local Law Enforcement Contact Information (phone/email): Phone E-mail
6. Has the FBI been Notified: (If yes, fill out #s C7-8): ☐ Yes ☐ No	7. FBI Agent Name: (First M. Last) First MI Last	
8. FBI Agent Contact Information (phone/email): Phone E-mail		
9. Was the stolen BSAT material recovered: ☐ Yes ☐ No	10. Was there a potential exposure: (If yes, go to section E- Q: 5-11) ☐ Yes ☐ No ☐ Unsure	

Certification: I hereby certify that the information contained on this form is true and correct to the best of my knowledge. I understand that if I knowingly provide a false statement on any part of this form, or its attachments, I may be subject to criminal fines and/or imprisonment. I further understand that violations of the select agent regulations may result in civil or criminal penalties, including imprisonment. 7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73.

Signature of Respondent: _____

Title: _____

Typed or printed name of Respondent: _____

Date: _____

Incident Notification and Reporting Form

SECTION D - REPORT OF LOSS			
1. Type of Loss: ☐ Inventory/Recordkeeping error ☐ Sample lost/discarded at entity ☐ Sample lost in transit (Go to Appendix B to enter add'l info) ☐ Other: _____	2. Has Local Law Enforcement been Notified: (If yes, fill out #s D3-D5) ☐ Yes ☐ No	3. Local Law Enforcement Agency: 	
4. Local Law Enforcement Agent Name: _____ _____ _____ First MI Last		5. Local Law Enforcement Contact Information (phone/email): _____ _____ Phone E-mail	
6. Was the FBI Notified: (If yes, fill out #s D7-D8) ☐ Yes ☐ No	7. FBI Agent Name: _____ _____ First MI _____ _____ Last		8. FBI Agent Contact Information (phone/email): _____ Phone _____ E-mail
9. Was the lost BSAT material found? ☐ Yes ☐ No	10. How long was the BSAT material missing? Duration of loss (hrs/days): _____ Date recovered: _____	11. Give the date of the last inventory/audit performed, which meets the FSAP regulatory requirement: _____	12. Was there a potential exposure: (If yes, complete Section E- Q: 5-11) ☐ Yes ☐ No

Certification: I hereby certify that the information contained on this form is true and correct to the best of my knowledge. I understand that if I knowingly provide a false statement on any part of this form, or its attachments, I may be subject to criminal fines and/or imprisonment. I further understand that violations of the select agent regulations may result in civil or criminal penalties, including imprisonment. 7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73.

Signature of Respondent: _____

Title: _____

Typed or printed name of Respondent: _____

Date: _____

Incident Notification and Reporting Form

SECTION E- REPORT OF RELEASE														
1. Type of Potential Exposure/Release: (choose all that apply) <table border="0"><tr><td>☐ Animal bite/scratch</td><td>☐ Equipment/mechanical failure</td></tr><tr><td>☐ PPE failure</td><td>☐ Package damaged in transit (fill out Appendix B)</td></tr><tr><td>☐ Spill</td><td>☐ Unintended Animal Infection</td></tr><tr><td>☐ Needle stick/Sharps</td><td>☐ Unintended Plant Pathogen Release</td></tr><tr><td>☐ Decontamination failure</td><td>☐ Work performed on an open bench</td></tr><tr><td>☐ Inactivation failure</td><td>☐ Other: _____</td></tr></table>		☐ Animal bite/scratch	☐ Equipment/mechanical failure	☐ PPE failure	☐ Package damaged in transit (fill out Appendix B)	☐ Spill	☐ Unintended Animal Infection	☐ Needle stick/Sharps	☐ Unintended Plant Pathogen Release	☐ Decontamination failure	☐ Work performed on an open bench	☐ Inactivation failure	☐ Other: _____	2. Was there a release outside containment barriers? (choose all that apply) ☐ Release outside primary containment (e.g., biosafety cabinet, leaking storage vial within storage unit) ☐ Release beyond secondary containment (e.g., laboratory) ☐ Release outside all containment barriers of the facility (e.g., resulting in possible agricultural/environmental/ public health threat)
☐ Animal bite/scratch	☐ Equipment/mechanical failure													
☐ PPE failure	☐ Package damaged in transit (fill out Appendix B)													
☐ Spill	☐ Unintended Animal Infection													
☐ Needle stick/Sharps	☐ Unintended Plant Pathogen Release													
☐ Decontamination failure	☐ Work performed on an open bench													
☐ Inactivation failure	☐ Other: _____													
3. What PPE was worn at the time of the incident? (choose all that apply) <table border="0"><tr><td>☐ Hand Protection (e.g., gloves)</td><td>☐ Foot Protection (e.g., boots, shoe covers)</td></tr><tr><td>☐ Head Protectors/Covers</td><td>☐ Eye/Face Protection (e.g., goggles, face shield)</td></tr><tr><td>☐ Body Protection</td><td>☐ Respiratory Protection Type: _____</td></tr><tr><td colspan="2">☐ Other/None: _____</td></tr></table>		☐ Hand Protection (e.g., gloves)	☐ Foot Protection (e.g., boots, shoe covers)	☐ Head Protectors/Covers	☐ Eye/Face Protection (e.g., goggles, face shield)	☐ Body Protection	☐ Respiratory Protection Type: _____	☐ Other/None: _____		4. Did the release result in potential exposure(s)? ☐ Yes If yes, how many individuals/animals/plants were exposed? _____ ☐ No				
☐ Hand Protection (e.g., gloves)	☐ Foot Protection (e.g., boots, shoe covers)													
☐ Head Protectors/Covers	☐ Eye/Face Protection (e.g., goggles, face shield)													
☐ Body Protection	☐ Respiratory Protection Type: _____													
☐ Other/None: _____														
5. Did the release result in a laboratory acquired infection or an infection/outbreak in agriculture or in the environment? ☐ Yes ☐ No ☐ Not currently known	6. Has medical surveillance been initiated? ☐ Yes _____ ☐ No	7. Has prophylaxis or treatment been provided? ☐ Yes ☐ No												
8. Has an internal investigation been initiated to lessen the likelihood of recurrences of incident involving the select agents and toxins at this entity? ☐ Yes (If yes, please provide additional details.) ☐ No _____														
9. Other than a potential for occupational illness, what other hazards have been identified as a result of this incident? _____														
10. Provide a brief summary of how the laboratory and work surfaces were decontaminated after the incident. _____														
11. Provide a brief summary of the medical surveillance conducted (do not provide names or confidential information). _____														

Certification: I hereby certify that the information contained on this form is true and correct to the best of my knowledge. I understand that if I knowingly provide a false statement on any part of this form, or its attachments, I may be subject to criminal fines and/or imprisonment. I further understand that violations of the select agent regulations may result in civil or criminal penalties, including imprisonment. 7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73.

Signature of Respondent: _____

Title: _____

Typed or printed name of Respondent: _____

Date: _____

APPENDIX A

EVENTS TIMELINE

Provide a detailed summary of events, including a timeline of what occurred.

Incident Notification and Reporting Form

APPENDIX B IF THE INCIDENT OCCURRED DURING TRANSFER, COMPLETE SECTIONS A AND B OF FORM 3 AND PROVIDE THE FOLLOWING INFORMATION (INCLUDE A COPY OF THE RELEVANT APHIS/CDC FORM 2)	
1. Transfer authorization number from APHIS/CDC Form 2:	2. Date Shipped
3. Name of Carrier	4. Airway bill number, bill of lading number, tracking number
5. Package Description (size, shape, description of packageing including number and type of inner packages; attach additional sheets as necessary)	
6. Package with select agents and toxins received by requestor: ☐ No ☐ Yes If yes, date of receipt: _____	7. Package with select agents and toxins appears to have been opened or damaged during shipment: ☐ No ☐ Yes If yes, include explanation in box 5 above.
8. Sender was contacted regarding incident: ☐ No ☐ Yes	9. Carrier/courier was contacted regarding incident: ☐ No ☐ Yes

Certification: I hereby certify that the information contained on this form is true and correct to the best of my knowledge. I understand that if I knowingly provide a false statement on any part of this form, or its attachments, I may be subject to criminal fines and/or imprisonment. I further understand that violations of the select agent regulations may result in civil or criminal penalties, including imprisonment. 7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73.

Public reporting burden: Public reporting burden of providing this information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to CDC/ATSDR Reports Clearance Officer, 1600 Clifton Road NE, MS D74, Atlanta, Georgia 30329; ATTN: PRA (0920-0576).

Signature of Respondent: _____

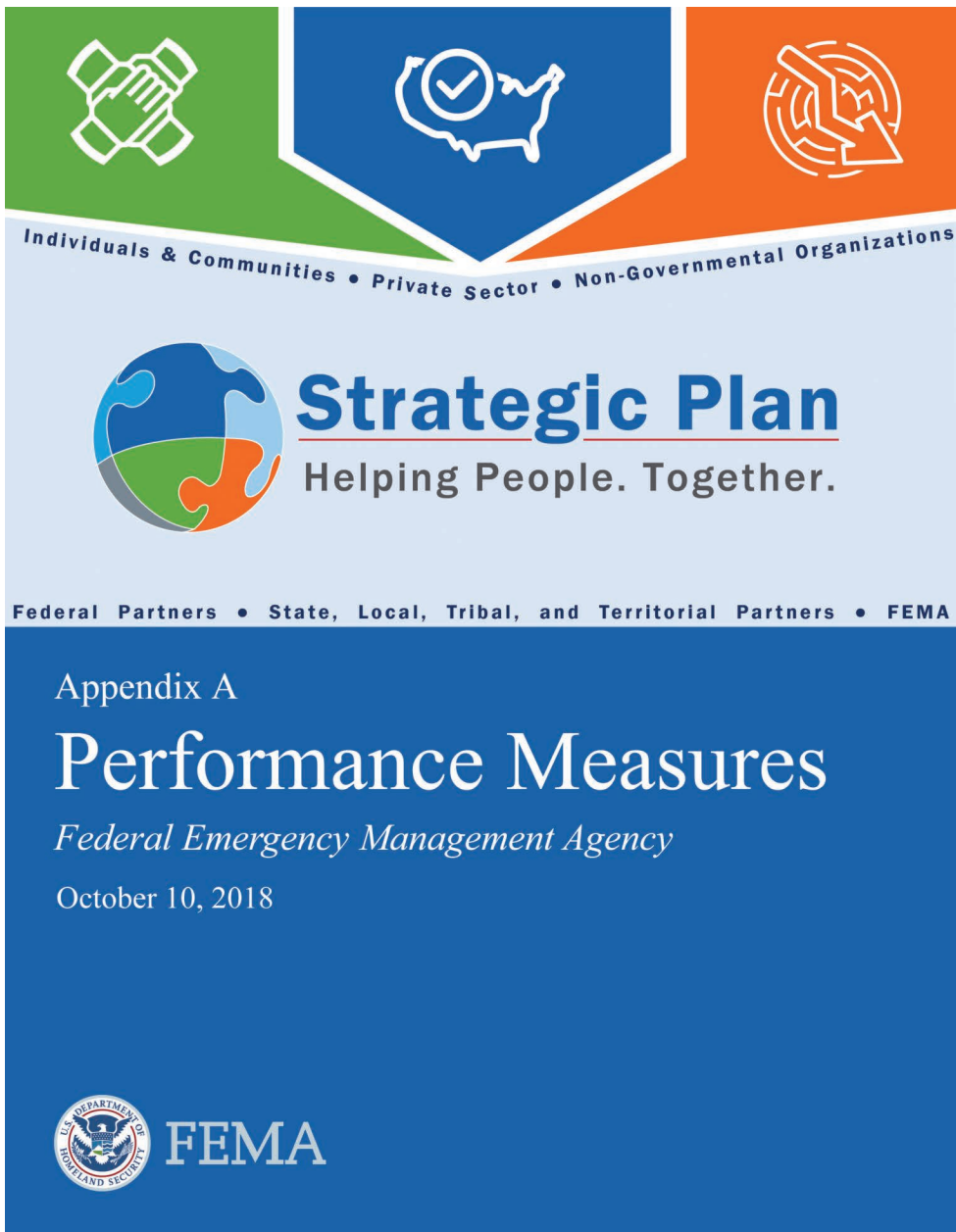
Title: _____

Typed or printed name of Respondent: _____

Date: _____

Appendix E

FEMA Strategic Plan Performance Measures



FEMA Strategic Plan Performance Measures



Strategic Goal 1: Build a Culture of Preparedness

Objective 1.1 Performance Measure:

Implement the National Mitigation Investment Strategy by quadrupling the investment in mitigation. *Data Source: MitInvest*

Baseline	2018	2019	2020	2021	2022
\$0.99 B	\$1.39 B	\$1.66 B	\$2.00 B	\$2.40 B	\$3.96 B

Objective 1.2 Performance Measure:

Double the number of properties covered by flood insurance through the private sector or the government.

Data Source: Transaction Record Reporting and Processing/PIVOT, National Association of Insurance Commissioners

Baseline	2018	2019	2020	2021	2022
4 Million	4.20 M	4.50 M	5.00 M	5.50 M	8.0 M

Objective 1.3 Performance Measures:

FEMA and stakeholder partners will improve financial literacy in the U.S. by achieving a 16 percentage point increase above the 2018 baseline of respondents who answer that they have set aside money for emergencies. *Data Source: FEMA National Household Survey*

Baseline	2019	2020	2021	2022
TBD	Baseline + 4%	Baseline + 8%	Baseline + 12%	Baseline + 16%

To build the capacity and resilience of community-based organizations, a total of 22,000 organizations will receive training from FEMA and its partners, with 65% reporting they have taken action with disaster continuity planning. *Data Source: FEMA Database*

Baseline	2019	2020	2021	2022
0	5,500	11,000	16,500	22,000

Baseline	2019	2020	2021	2022
TBD	65%	65%	65%	65%

Increase the percentage of National Household Survey respondents who have taken three or more preparedness actions.

Data Source: FEMA National Household Survey

Baseline	2018	2019	2020	2021	2022
46%	47%	48%	49%	50%	51%

Objective 1.4 Performance Measures:

Increase the number of FEMA employees who say they “feel encouraged to come up with new and better ways of doing things” on the Federal Emergency Viewpoint Survey (FEVS) by 10 percentage points. *Data Source: FEVS*

Baseline	2018	2019	2020	2021	2022
60%	62%	64%	66%	68%	70%

The Nation will show an improvement on 25% of the targets identified in the annual Stakeholder Preparedness Review (SPR). *Data Source: SPR*

Baseline	2020	2021	2022
TBD	8%	17%	25%



Strategic Goal 2: Ready the Nation for Catastrophic Disasters

Objective 2.1 Performance Measures:

Designate 20,000 personnel as fully qualified by authorities having jurisdiction in the National Qualification System.

Data Source: OneResponder System, Deployment Tracking System

Baseline	2018	2019	2020	2021	2022
0	250	5,000	10,000	15,000	20,000

FEMA will improve the readiness of its incident workforce cadres from a D3 (60-74%) to a D2 (75-89%) rating of overall readiness. *Data Source: Cadre Operational Readiness and Deployability Status Report*

Baseline	2018	2019	2020	2021	2022
D3 (64%)	65%	68%	70%	72%	D2 (75%)

Demonstrate a Unified National Incident Workforce through the efficient deployment of non-FEMA personnel at the same rate as FEMA personnel during 100% of presidentially-declared events. *Data Source: FEMA Deployment Tracking System*

Baseline	2018	2019	2020	2021	2022
0%	20%	40%	60%	80%	100%

Objective 2.2 Performance Measures:

Increase the number of partners participating in the FEMA Integration Teams program. *Data Source: FEMA Integration Team Resource Tracker*

Baseline	2018	2019	2020	2021	2022
0	10	34	56	61	65

Decrease the five year average amount of Federal incident workforce that supports small federally-declared disasters. *Data Source: FEMA Deployment Tracking System*

Baseline	2018	2019	2020	2021	2022
93	93	93	93	93	93

Objective 2.3 Performance Measures:

Build FEMA staff, equipment, and contract capacity to achieve and maintain a 93% composite logistics readiness rate for moving, staging, and delivering commodities and equipment for catastrophic disasters. *Data Source: Logistics Supply Chain Management System*

Baseline	2018	2019	2020	2021	2022
TBD	93%	93%	93%	93%	93%

Update 100% of Regional and National Catastrophic Plans to include an effective private sector Supply Chain Integration Appendix in alignment with the FEMA Private Sector Supply Chain Management Plan published in FY 2018.

Data Source: FEMA Deployment Tracking System

Baseline	2019	2020	2021	2022
0	23%	45%	75%	100%

FEMA Strategic Plan Performance Measures



Strategic Goal 2: Ready the Nation for Catastrophic Disasters

Objective 2.3 Performance Measures (continued):

FEMA will work with states and territories to ensure that all 56 have effective distribution management plans integrated with FEMA resource support strategies. *Data Source: FEMA Database*

Baseline	2019	2020	2021	2022
0	10	20	35	45

Objective 2.4 Performance Measures:

Increase the percentage of states and territories with comprehensive continuity plans and programs for state agencies and emergency operations centers that align with the Continuity Guidance Circular (CGC), to ensure the continuation of their essential functions under all conditions. *Data Source: Continuity Assessment Tool (CAT)*

Baseline	2018	2019	2020	2021	2022
0	1.8%	19.6%	37.5%	55.3%	73%

Increase the percentage of critical Federal response teams that Disaster Emergency Communications can support with voice, video, and data connectivity using a fully capable mobile emergency office vehicle. *Data Source: FEMA MEOV Inventory*

Baseline	2018	2019	2020	2021	2022
75%	78%	81%	84%	88%	90%

Update State, Tribal, Territorial Communications Plans with essential information on continuity communications, resilience, and other critical lifeline elements to ensure that emergency responders, and those who support them, can act on lifesaving/life sustaining information during catastrophic events. *Data Source: FEMA Database*

Baseline	2018	2019	2020	2021	2022
0	10.7%	21.4%	32.1%	42.9%	53.6%



Strategic Goal 3: Reduce the Complexity of FEMA

Objective 3.1 Performance Measures:

Decrease the percentage of FEMA and overall Federal in-person inspections. *Data Source: National Emergency Management Information Systems, FEMA's Operations Data Storage Database*

Baseline	2019	2020	2021	2022
100%	91.7%	64%	60.7%	57.4%

Raise applicant satisfaction with the simplicity of the Individuals and Households Program Process. *Data Source: FEMA's WinCATI System*

Baseline	2018	2019	2020	2021	2022
76.8%	79%	81%	83%	85%	87%

Raise applicant satisfaction with the simplicity of the Public Assistance Process. *Data Source: FEMA's WinCATI System*

Baseline	2018	2019	2020	2021	2022
78.5%	80%	82%	84%	86%	88%

Increase the timeliness of financial assistance awards of the Individuals and Households Program. *Data Source: National Emergency Management Information System, FEMA's Operations Data Storage Database*

Baseline	2018	2019	2020	2021	2022
12.9 days	13 days	11 days	9 days	8 days	7 days

Increase the timeliness of financial assistance awards of the Public Assistance Program. *Data Source: National Emergency Management Information System, FEMA's Operations Data Storage Database*

Baseline	2018	2019	2020	2021	2022
62%	64%	68%	72%	74%	75%

Improve the accuracy of financial assistance of the Individuals and Households Program. *Data Source: National Emergency Management Information System, FEMA's Operations Data Storage Database*

Baseline	2018	2019	2020	2021	2022
95.8%	95%	95.5%	96%	96.5%	97%

Improve the accuracy of financial assistance of the Public Assistance Program. *Data Source: National Emergency Management Information System, FEMA's Operations Data Storage Database*

Baseline	2018	2019	2020	2021	2022
89.5%	89.5%	90%	90.5%	91%	91.5%

Objective 3.2 Performance Measures:

Improve the recovery capability of states and territories by increasing:

- The number of States and territories with pre-designated State Disaster Recovery Coordinators or equivalent, and
- The number of pre-disaster recovery plans based upon the principles of the National Disaster Recovery Framework.

Data Source: TBD

Baseline	2018	2019	2020	2021	2022
TBD	TBD	TBD	TBD	TBD	TBD

FEMA Strategic Plan Performance Measures



Strategic Goal 3: Reduce the Complexity of FEMA

Objective 3.2 Performance Measures: (Continued)

Using the 2017 Federal Interagency Recovery Readiness Assessment results as a baseline, FEMA will partner with the interagency to strengthen recovery capability, as measured by the baseline readiness index, increasing scores by 25%.

Data Source: Interagency Recovery Readiness Assessment

Baseline	2019	2021	2023
46.2%	50.1%	53.9%	57.8%

Objective 3.3 Performance Measures:

FEMA will focus on efficient and effective program delivery by decreasing the number of repeat audit findings through the simplification, standardization and streamlined governance of business processes. *Data Source: A-123 Summary of Aggregate Deficiencies*

Baseline	2018	2019	2020	2021	2022
100%	80%	59%	39%	20%	0%

Reflecting a commitment to its workforce, FEMA will increase the Global Satisfaction, Employee Engagement, and Diversity Indices by 10 percentage points each. *Data Sources: Federal Employee Viewpoint Survey (FEVS)*

Baseline Global	2018	2019	2020	2021	2022
63.3%	65.3%	67.3%	69.3%	71.3%	73.3%

Baseline Engagement	2018	2019	2020	2021	2022
66.4%	68.4%	70.4%	72.4%	74.4%	76.4%

Baseline Diversity	2018	2019	2020	2021	2022
58.8%	60.8%	62.8%	64.8%	66.8%	68.8%

To enhance cybersecurity across the Agency, FEMA will achieve and maintain a rating of “green” on the Federal Information Security Modernization Act metrics through modernization, system consolidation, decommissioning, and business process reengineering. *Data Source: Federal Information Security Modernization Act (FISMA) Scorecard*

Baseline	2018	2019	2020	2021	2022
56%	65%	75%	85%	90%	95%

Objective 3.4 Performance Measures:

Improve recipients’ capability to monitor sub-recipients through development of internal controls and targeted technical assistance opportunities by reducing the percentage of questioned costs by the Office of Inspector General by five percentage points. *Data Source: FEMA System of Record*

Baseline	2018	2019	2020	2021	2022
19%	18%	15%	13%	11%	5%

To strengthen grants management across the Agency, remediate 90% of repeat FEMA grants-related financial statement audit findings and recommendations. *Data Source: Notice of Findings & Recommendations, DHS Consolidated Financial Audit*

Baseline	2018	2019	2020	2021	2022
100%	83%	67%	50%	33%	0%



Strategic Goal 3: Reduce the Complexity of FEMA

Objective 3.4 Performance Measure(s) (continued):

Establish a consistent process for completing grant closeout to reduce the number of grants overdue for closeout by 80% in accordance with the Grants Oversight and New Efficiency (GONE) Act. *Data Source: FEMA's Web Integrated Financial Management Information System*

Baseline	2018	2019	2020	2021	2022
809	85% closed	100% closed	New Measure TBD	New Measure TBD	New Measure TBD

To increase transparency in FEMA's stewardship of taxpayer funds, FEMA will make datasets on the amount and purpose of all funds provided to SLTT and other Federal agencies publicly available and machine readable. *Data Source: FEMA's Web Integrated Financial Management Information System*

Baseline	2018	2019	2020	2021	2022
53%	58%	72%	78%	84%	90%



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

- 1st Information Operations (IO) Command 337
- 2007 Homeland Security reauthorization 113
- 9/11 Commission 47, 410
- 9/11 Commission Act of 2007 633
- A&M *see* Air and marine (A&M) based program (A&M)
- AAR *see* After action report (AAR)
- ACS *see* Automated Commercial System (ACS)
- ADAC *see* Arctic Domain Awareness Center of Excellence (ADAC)
- advanced imaging technology (AIT) 498
- advanced radiography 136
- advanced spectroscopic portal systems 139
- AFG *see* Assistance to Firefighters Grant
- Afghanistan 14, 219, 322, 329, 419
- AFSC *see* Army Field Support Center (AFSC)
- after-action report (AAR) 265
- Agricultural Research Service (ARS) 578
- agriculture
 - food 569
 - infectious animals 578
 - infectious diseases and bioterrorism 581
 - National Select Agent Registry Program 588
 - Project BioShield 587
 - Strategic National Stockpile 588
 - Strategic Partnership Program on
 - Agroterrorism 575
- agroterrorism 575
- AI *see* Bird flu
- air and marine (A&M)-based program (A&M) 446
- Air Force Intelligence, Surveillance, and Reconnaissance Agency 334
- AIT *see* Advanced imaging technology
- ALERT *see* Center of Excellence for Awareness and Localization of Explosives-Related Threats (ALERT)
- Al-Qaeda 29
- American Civil Liberties Union 103
- American Red Cross 197
- Amtrak 260, 534, 542–544
- Animal and Plant Health Inspection Service (APHIS) 579
- anthrax 202, 581
- AOG *see* Army Operations Group (AOG)
- APHIS *see* Animal and Plant Health Inspection Service (APHIS)
- Arctic Domain Awareness Center of Excellence (ADAC) 632
- Area Maritime Security Committees 521
- Arms and Strategic Technology 472
- Army Field Support Center (AFSC) 338
- Army Operations Group (AOG) 338
- ARS *see* Agricultural Research Service (ARS)
- Assistance to Firefighters Grant (AFG) 259
- asylum 56
- ATF *see* Bureau of Alcohol, Tobacco, and Firearms (ATF)
- ATR *see* Automated target recognition (ATR)
- atropine 213
- ATS *see* Automated targeting systems (ATS)
- Aum Shinrikyo 212
- Automated Commercial Environment (ACE) program 459
- Automated Commercial System (ACS) 458
- automated targeting systems (ATS) 125
- automated target recognition (ATR) 500
- AVIP *see* Anthrax Vaccine Immunization Program (AVIP)
- Bacillus anthracis* 201
- backscatter technology 499
- BARDA *see* Biomedical Advanced Research and Development Authority (BARDA)
- Barr, William 109
- Bauer, Alain 188
- BCE *see* Bovine spongiform encephalopathy (BCE)
- Beagle Brigade 581
- Berlin Airlift 8
- biological agents 198–202
- biological weapons
 - anthrax 202, 581
 - generally 198–206
 - plague 204
 - smallpox 206
- Biomedical Advanced Research and Development Authority (BARDA) 587
- biometrics
 - Registered Traveler (RT) program 502
 - TSA paperless boarding pass 508
 - use of 113, 475, 501
- Biometric Support Center 113
- BioShield 121, 127, 587
- bioterrorism
 - definition 585
 - generally 581–589
- BioWatch program 146, 198
- bird flu 590
- Black Panthers 22
- Blair, Dennis 414
- Blanco, Kathleen 381
- Border and Marine Division 512
- Border Patrol 430–476
- Border Protection, Antiterrorism, and Illegal Immigration Control Act 462
- border wall 38, 51, 158–163, 441
- Boston Marathon Bombing 26
- bovine spongiform encephalopathy (BCE) 578
- BSC *see* Biometric Support Center (BSC)
- bubonic plague 205
- Building Security Committee 69
- Bureau of Alcohol, Tobacco, and Firearms (ATF) 296, 401
- Bureau of Public Roads 351
- Bush, George W., 46, 94, 106, 409
- Business Outreach Group 236

Index

- C3 *see* Cyber Crimes Center
CAMRA *see* Center for Advancing Microbial Risk Assessment (CAMRA)
canine explosive detection unit 493
CanScan project 512
CAOCL *see* Center for Advanced Operational Culture Learning (CAOCL)
cargo
 Automated Commercial Environment 459
 Container Security Initiative 123, 455
 Customs-Trade Partnership against Terrorism (C-TPAT) 125, 457
 and ports 136, 432, 526
 Secure Freight Initiative (SFI) 451–455
Cargo Advanced Automated Radiography Systems 136
Carnegie Mellon University 226
Carter, Jimmy 14, 352
CARVER+Shock assessment tool 180
castor beans 210
CBP *see* Customs and Border Protection (CBP)
CBPO *see* Customs and Border Protection Officer (CBPO)
CBR *see* Chemical, biological, or radiological (CBR) contamination
CBRN *see* Chemical, biological, radiological, and nuclear (CBRN) incident
CDC *see* Centers for Disease Control and Prevention
CDP *see* Center for Domestic Preparedness (CDP)
Center for Advanced Operational Culture Learning (CAOCL) 336
Center for Advancing Microbial Risk Assessment (CAMRA) 633
Center for Borders, Trade, and Immigration Research (CBTIR) 632
Center for Disaster Philanthropy 357
Center for Domestic Preparedness (CDP) 260
Center for Maritime, Island and Remote and Extreme Environment Security (MIREES) 633
Center for Security Evaluation 419
Center for Visualization and Data Analytics (CVADA) 632
Center of Excellence for Awareness and Localization of Explosives-Related Threats (ALERT) 632
Centers for Disease Control and Prevention (CDC) 121, 197, 251, 585, 603
Central America 430, 443, 462
Central Intelligence Agency
 Directorate of Analysis 410
 Directorate of Digital Innovation (DDI) 412
 Directorate of Science and Technology 412
 Directorate of Support 413
 generally 10, 41, 109, 409
 mission centers 413
 office of Clandestine Services 412
Central MASINT Office (CMO) 404
chain migration 467
CHC *see* Coastal Hazards Center of Excellence (CHC)
chemical, biological, or radiological (CBR)
 contamination 567
chemical, biological, radiological, and nuclear (CBRN) incident 345
Chemical, Ordnance, Biological, and Radiological Training Facility (COBRATF) 260
chemical facilities 113
chemical terror 208, 588
chemical weapons
 generally 206
 nerve agents 210
 ricin 210
Chertoff, Michael 52, 391
Chicago biological attack 197
Christmas Day Bombing 53
Churchill, Winston 7
CI *see* Counterintelligence (CI)
CIA *see* Central Intelligence Agency (CIA)
CIRI *see* Critical Infrastructure Resilience Institute (CIRI)
CISA *see* Cybersecurity and Infrastructure Security Agency (CISA)
CITAT *see* Container Inspection Training and Assist Team (CITAT)
Citizen Corps 320
Citizenship and Immigration Services
 Ombudsman 56
civil cooperation 325, 326, 327
Civil Maritime Intelligence Division 331
Civil Support Teams (CSTs) 341
Clovis, Samuel, Jr., 630
CMO *see* Central MASINT Office (CMO)
Coastal Hazards Center of Excellence (CHC) 633
Coastal Resilience Center of Excellence (CRC) 632
COBRATF *see* Chemical, Ordnance, Biological, and Radiological Training Facility (COBRATF)
Cold War 6
Community Emergency Response Teams 272
Communist Workers Party 26
Compliance and Technical Assistance Branch 275
computer security
 information infrastructure 222
 National Cyber Security Division 228
 US-CERT 223, 229
Congressional Research Service 370
Consortium of National Academies 219
Container Inspection 525
Container Inspection Training and Assist Team (CITAT) 524
Container Security Device (CSD) 512
Container Security Initiative (CSI) 123, 455
Cornerstone Initiative 471
coronavirus
 FEMA response 357
 generally 565, 571, 590, 595–602
 health sector response 602–611
 presidential actions 55, 63, 67
Cotton, Tom 159
counterfeit passport card 472
counterintelligence (CI) 396, 418
Counter Narcotics Enforcement 57
Counter-Proliferation Investigations Program 434
counterterrorism 41, 396, 403, 417, 521, 627
Counterterrorism and Criminal Exploitation Unit 434
COVID-19 *see* Coronavirus
CRC *see* Coastal Resilience Center of Excellence (CRC)

- CREATE *see* National Center for Risk and Economic Analysis of Terrorism Events (CREATE)
- Critical Infrastructure and Resilience Month 94
- Critical Infrastructure Partnership Advisory Council 102
- Critical Infrastructure Protection Month 94
- Critical Infrastructure Resilience Institute (CIRI) 632
- Critical Infrastructure Security and Resilience 102, 564
- CSD *see* Container Security Device (CSD)
- CSI *see* Container Security Initiative (CSI)
- CSTs *see* Civil Support Teams (CSTs)
- CSX 544
- CSXT *see* CSX Transportation (CSXT)
- CSX Transportation (CSXT) 544
- C-TPAT *see* Customs-Trade Partnership against terrorism (C-TPAT)
- Customs and Border Protection (CBP) 430, 577
- Customs and Border Protection Officer (CBPO) 113
- Customs and immigration Service 465
- Customs-Trade Partnership against Terrorism (C-TPAT) 125, 457
- cyber attacks 223, 567, 623
- Cyber Crimes Center 472
- cybersecurity 63, 94, 115, 222, 320
- Cybersecurity and Infrastructure Security Agency (CISA) 63–66
- Cyber Storm 65, 229
- cyberterrorism 129
- Cyber Warning and Information Network 226
- Daily Brief 410
- dam infrastructure 369
- DDI *see* Directorate of Digital Innovation (DDI)
- Decentralized Model 629
- Defend America program 331
- Defense Attaché System 424
- Defense Authorization Bill 103
- Defense HUMINT Service 424
- Defense Intelligence Agency (DIA) 423
- Defense Intelligence Analysis Center 423
- Defense Threat Reduction Agency (DTRA) 343
- Deferred Action for Childhood Arrivals (DACA) 464–467
- demilitarized zone 20
- Department of Commerce 238, 481
- Department of Defense (DoD) 106, 327
- Department of Energy (DOE) 139, 454, 565
- Department of Health and Human Services (HHS) 120
- Department of Homeland Security (DHS)
- evolution 46
 - genesis of 38
 - national vs. homeland 289–322
 - reorganization of 49
 - secretary of 51
 - strategic plan 46, 79, 85, 297, 627
- Department of Justice (DOJ) 41
- Department of state (DOS) 467
- Designated Federal Officer (DFO) 640
- detention policy 102
- DFO *see* Designated Federal Officer (DFO)
- DFTO *see* Disaster Field Training Operations (DFTO) Program
- DHS *see* Department of Homeland Security (DHS)
- DHS Directorate on Science and Technology 51
- DHS Homeland Security Grant Program 259, 319
- DHS Preparedness Grant Program 259
- DIA *see* Defense Intelligence Agency (DIA)
- Directorate for Management 68
- Directorate for National Protection and Programs 63
- Directorate for Science and Technology 66
- Directorate of Digital Innovation (DDI) 412
- Directorate of Support 413
- Director of National Intelligence 414
- Dirty Bomb 196, 240, 407
- Disaster Field Training Operations (DFTO) Program 264
- DisasterAssistance.gov 362
- discussion-based exercises 267
- Diversity Immigrant Visa Program (DV Program) 467
- DNDO *see* Domestic Nuclear Detection Office (DNDO)
- DoD *see* Department of Defense (DoD)
- DOE *see* Department of Energy (DOE)
- DOJ *see* Department of Justice (DOJ)
- Domestic Nuclear Detection Office (DNDO) 73, 130, 131, 192
- Domestic Outreach Plan 511
- domestic terrorism 23–29, 253, 399
- DOS *see* Department of State (DOS)
- Drexel University 633
- driver's licenses 109
- drug enforcement 56
- DTRA *see* Defense Threat Reduction Agency (DTRA)
- Dunai, Daniel 185
- early warning system 358, 585
- earthquake design 369
- EAS *see* Emergency Alert System (EAS)
- Ebola crisis 56, 590
- Economics Group 236
- Electronic Surveillance 107, 132
- Emergency Alert System (EAS) 134, 358
- Emergency Management Institute 261
- Emergency Management Performance Grant (EMPG) 260
- Emergency Preparedness Directorate (EPD) 192
- Emergency Preparedness Project Office (EPPO) 192
- EMI Higher Education Conference 264
- EMPG *see* Emergency Management Performance Grant (EMPG)
- enterprise risk management (ERM) 496
- Environmental Protection Agency (EPA) 297, 565
- EPA *see* Environmental Protection Agency (EPA)
- EPD *see* Emergency Preparedness Directorate (EPD)
- EPPO *see* Emergency Preparedness Project Office (EPPO)
- ERM *see* Enterprise risk management (ERM)
- E-Verify 142, 143
- executive orders 94–104
- Export Enforcement Coordination Center 434
- FACA *see* Federal Advisory Committee Act (FACA)
- “Fast and Furious” operation 55
- FBI *see* Federal Bureau of Investigation (FBI)
- FCC *see* Federal Communications Commission (FCC)
- FDA *see* Food and Drug Administration

Index

- Federal Advisory Committee Act (FACA) 639
Federal Air Marshal Service 132, 491
Federal Bureau of Investigation
 generally 25, 38, 219, 396
 joint terrorism task forces 401, 543
 National Security Branch 403
Federal Communications Commission (FCC) 134
Federal Disaster Assistance Administration 352
Federal Emergency Management Agency (FEMA)
 historical foundation 352–357
 preparedness 357
 role of mitigation 367
 response and recovery 378
Federal Flight Deck Officers (FFDO) 491
Federal Insurance and Mitigation Administration
 (FIMA) 370
Federal Law Enforcement Training Center (FLETC)
 70, 83
Federal Protective Service (FPS) 68, 176
Federal Transit Administration 541
FEMA *see* Federal Emergency Management Agency
 (FEMA)
FFDO *see* Federal Flight Deck Officers (FFDO)
FIMA *see* Federal Insurance and Mitigation
 Administration (FIMA)
Fire Prevention and Safety (FP&S) 259
FISA *see* Foreign Intelligence Surveillance Act (FISA)
FLETC *see* Federal Law Enforcement Training Center
 (FLETC)
Flood Map Service Center 373
FloodSmart program 373
FOF *see* Force on Force (FOF) Training
Food and Drug Administration (FDA) 180, 570
Food Protection and Defense Institute (FPDI) 632
Food Safety and Inspection Service (FSIS) 576
Force on Force Training (FOF) 194
Foreign Intelligence Surveillance Act (FISA) 41
Fort Hood shootings 418
FP&S *see* Fire Prevention and Safety (FP&S)
FPDI *see* Food Protection and Defense Institute (FPDI)
FPS *see* Federal Protective Service
Freedom Act of 2015 107
Freedom of Information Act 83 641
Freeh, Louis 28
Freidman, Benjamin 636
FSIS *see* Food Safety and Inspection Service (FSIS)
Fugate, Craig 357, 366
Fugitive Operations Program 470
funding, and grant systems for DHS 256, 319, 632
future of homeland security 621

G&T *see* Office of Grants and Training (G&T)
GD *see* Soman
geographic information systems (GIS) 365
Germany 2–9
Giffords, Gabrielle 53
GIS *see* Geographic Information Systems (GIS)
Giuliani, Rudy 381
Global Corporate College 482
global entry program 60
Global Maritime Intelligence Integration Plan 511
Global Trade Exchange (GTX) 455

Gorbachev, Mikhail 12
government-centric approach 357, 624
great wave 460
GTX *see* Global Trade Exchange (GTX)
G-type agents 212
Guantanamo operations 103

H1N1 virus 590
H5N1 virus 592
Haitian Refugee Immigration and Fairness Act
 (HRIFA) 462
Hasan, Nidal Malik 418, 623
hazard mitigation 178, 378
Hazus software 263, 365
Heritage Foundation 464, 629
Heydrich, Reinhard 3
HHS *see* Department of Health and Human Services
 (HHS)
high-threat urban areas (HTUA) 260, 544
HSI *see* Homeland Security Investigations (HSI)
Hitler, Adolf 3, 213
HLT *see* Hurricane Liaison Team (HLT)
Holder, Eric 55
Homeland Security Act of 2002 47, 104
Homeland Security Advisory Council (HSAC) 297, 639
Homeland Security Advisory Warning System 123
Homeland Security Digital Library (HSDL) 270
Homeland Security Exercise and Evaluation Program
 (HSEEP) 250, 265
Homeland Security Grant Program (HSGP) 259, 319
Homeland Security Investigations (HSI) 437
Homeland Security Operations Center (HSOC) 134
Homeland Security Presidential Directives 229, 255,
 274, 566
Homeland Security Research Corporation 233
Hospital Preparedness Program (HPP) 586
hospitals, and medical facilities 275, 367, 380, 565, 586
HPP *see* Hospital Preparedness Program (HPP)
HRIFA *see* Haitian Refugee Immigration and Fairness
 Act (HRIFA)
HSAC *see* Homeland Security Advisory Council
 (HSAC)
HSDL *see* Homeland Security Digital Library (HSDL)
HSEEP *see* Homeland Security Exercise and Evaluation
 Program (HSEEP)
HSGP *see* Homeland Security Grant Program (HSGP)
HSOC *see* Homeland Security Operations Center
 (HSOC)
HTUA *see* High-threat urban areas (HTUA)
human intelligence (HUMINT) 390, 404, 423
Human Rights Violators and War Crimes Unit 434
HUMINT *see* Human Intelligence (HUMINT)
Hurricane Liaison Team (HLT) 370
Hybrid Composite Container project 513

IBSGP *see* Intercity Bus Security Grant Program (IBSGP)
ICE *see* Immigration and Customs Enforcement (ICE)
ICS *see* Incident Command System (ICS)
IDENT biometric watchlist 113
IED *see* Improvised Explosive device (IED)
IEMS *see* Integrated emergency management system
 (IEMS)

- “If You *see* Something, Say Something” campaign 487
 IG *see* Inspector General (IG)
 illegal immigration 58, 434–440, 519
 imagery intelligence (IMINT) 390, 404
 immigration 434, 460–470, 624, 632
 Immigration and Customs Enforcement (ICE) 71, 434
 Immigration and Naturalization Service (INS) 462
 Immigration Reform and Control Act (IRCA) 462
 Improvised Explosive Device (IED) 218, 498, 567
 Incident Command System (ICS) 382, 645
 Incident Management Systems Integration Division 274
 infectious animals 578–581
 infectious diseases, and bioterrorism 581–588
 influenza viruses 590
 Infrastructure Protection Program (IPP) 320
 INS *see* Immigration and Naturalization Service (INS)
 INSCOM *see* Intelligence and Security Command (INSCOM)
 Inspection and Compliance Directorate 522
 Inspector General (IG) 56, 142, 230
 Integrated Early Warning System (IPAWS) 358
 Integrated emergency management system (IEMS) 352
 intelligence cycle 390
 Intelligence and Security Command (INSCOM) 337
 intelligence gathering and sharing 331–340
 Interagency Maritime Security Policy Coordinating Committee 510
 Intercity Bus Security Grant Program (IBSGP) 260
 Intergovernmental Affairs 49
 International Outreach and Coordination Strategy 511
 International Standards Organization (ISO) 513
 international terrorism 29
 IO *see* 1st Information Operation (IO) Command
 IPAWS *see* Integrated Early Warning System (IPAWS)
 IPP *see* Infrastructure Protection Program (IPP)
 Iran
 generally 12–18, 190, 212
 sanctions against 104
 Iraq 15, 219, 322, 329, 420
 IRCA *see* Immigration Reform and Control Act (IRCA)
 ISIL *see* Islamic State of Iraq and the Levant (ISIL)
 ISIS *see* Islamic State of Iraq and Syria (ISIS)
 Islamic extremism 26
 Islamic State of Iraq and the Levant (ISIL) 7
 Islamic State of Iraq and Syria (ISIS) 7
 ISO *see* International Standards Organization (ISO)

 Jackson State University 633
 Japanese imperialism 5
 Jews, extermination 2
 jihadi motivation 23–26, 392, 399, 534, 622
 Johns Hopkins University 633
 Johnson, Jeh 55, 152, 622
 Joint Analysis Center 139
 Joint Terrorism Task Forces (JTFFs) 25, 401, 543
 JTFFs *see* Joint Terrorism Task Forces (JTFFs)

 Kaczynski, Theodore (Ted) 26–29
 Katrina, Hurricane 106, 141, 252, 365–381
 Kelly, John 57
 Khrushchev, Nikita 12
 Kim Jong-Un 19

 King, Martin Luther, Jr., 22
 King Air (KA)-350CER 151
 Krebs, Chris 228
 Ku Klux Klan (KKK) 22–24, 31

 law enforcement officers 151, 486, 493, 546
 Law Enforcement Terrorism Prevention Program (LETPP) 320
 Lebanon, attack in 29
 Legal Immigration Family Equity (LIFE) Act 462
 Lessons Learned Information Sharing (LLIS) Program 250, 270
 LETPP *see* Law Enforcement Terrorism Prevention Program (LETPP)
 LIFE *see* Legal Immigration Family Equity (LIFE) Act
 LLIS *see* Lessons Learned Information Sharing (LLIS) Program
 London transit bombing 534
 Lowenthal, Mark M., 393

 McAleenan, Kevin K., 58
 McGinley, Ian Patrick 235
 McVeigh, Timothy 26, 221
 MAP MOD program 373
 Marine Asset Tag Tracking System (MATTS) 512
 Marine Corps University 336
 Marine Operations Coordination (MOC) plan 508
 Maritime Commerce Security Plan 511
 Maritime Infrastructure Recovery Plan 511
 Maritime Law Enforcement Academy 519
 Maritime Operational Threat Response (MOTR) program 509
 maritime security 67, 509–534
 Maritime Security Act of 2002 525
 Maritime Security Center of Excellence (MSC) 632
 Maritime Security Response Team (MSRT) 521
 Maritime Security Transportation Act of 2002 509
 Maritime Stewardship Council 75
 Maritime Transportation System (MTS) Security Plan 512
 MASINT *see* measurements and signatures intelligence (MASINT)
 MATs *see* Mitigation Assessment Teams (MATs)
 MATTS *see* Marine Asset Tag Tracking System (MATTS)
 measurement and signatures intelligence (MASINT) 404
 megaports 454
 Michigan State University 633
 Millimeter Wave device 498
 Minnesota Municipalities Utilities Association 278
 MIREES *see* Center for Maritime, Island and Remote and Extreme Environment Security (MIREES)
 mitigation 141, 171–179, 367–378
 Mitigation Assessment Teams (MATs) 370
 MOC *see* Marine Operations Coordination (MOC) plan
 MOTR *see* Maritime Operational Threat Response (MOTR) program
 MSC *see* Maritime Security Center of Excellence (MSC)
 MSRT *see* Maritime Security Response Team (MSRT)
 MTS *see* Maritime Transportation System (MTS) Security Plan

Index

- NACARA *see* Nicaraguan Adjustment and Central American Relief ACT (NACARA)
- Nagin, Ray 379, 381
- Napolitano, Janet 53–55, 185
- National Advisory Council 353
- National Advisory System 123
- National Biodefense Analysis and Countermeasures Center (NBACC) 122
- National Bulk Cash Smuggling Center 471
- National Capital Region Air Defense program 134, 135
- National Center for Border Security and Immigration (NCBSI) 633
- National Center for Medical Intelligence 423
- National Center for Risk and Economic Analysis of Terrorism Events (CREATE) 632
- National Center for the Study of Preparedness and Catastrophic Event Response (PACER) 633
- National Child Victim Identification System 472
- National Clandestine Service (NCS) 412
- National Commission on 9/11, 38, 47, 410, 633
- National Consortium for the Study of Terrorism and Responses to Terrorism (START) 632
- National Counterintelligence and Security Center (NCSC) 418
- National Counterintelligence Office 409
- National Counterterrorism Center (NCTC) 395, 417
- National Cyber Incident Response Plan (NCIRP) 258
- National Cyber Security Center 51
- National Cyber Security Division (NCSD) 129, 228
- National Cybersecurity and Communications Integration Center 63
- National Cyberspace Response System 228
- National Dam Safety Program (NDSP) 369
- National Defense Industrial Association (NDIA) 235
- National Domestic Preparedness Consortium 255
- National Earthquake Hazards Reduction Plan (NEHRP) 368
- National Emergency Responder Credentialing System 276
- National Exercise Program (NEP) 197, 256
- National Flood Insurance Program (NFIP) 352, 370, 629
- National Fugitive Operations Program (NFOP) 470
- National Governors' Association (NGA) Center for Best Practices 290
- National Ground Intelligence Center (NGIC) 338
- National Guard 106, 293, 322
- National Incident Management System (NIMS) 127, 274, 320, 643
- National Infrastructure Advisory Council 233
- National Infrastructure Protection Plan (NIPP) 141, 320
- National Institute of Health 595
- National Integration Center (NIC) 274
- National Intelligence Council 420
- National Intelligence officers (NIOs) 422
- National Intelligence Strategy 419
- National Level Exercise (NLE) 256
- National Maritime Intelligence-Integration Office (NMIO) 340
- National Monuments Agency 626
- National Nuclear Security Administration (NNSA) 454
- National Pharmaceutical Stockpile (NPS) 121, 588
- National Plan to Achieve Maritime Domain Awareness 512
- National Preparedness Annual Training and Exercise Conference 264
- National Preparedness Directorate (NPD) 357
- National Preparedness Goal 141
- National Preparedness Integration program 134
- National Reconnaissance Office (NRO) 340
- National Research Council 219
- National Response Framework (NRF) 282, 320, 380
- National Security Agency (NSA) 47, 109
- National Security Branch (NSB) 403
- National Security Council 546
- National Security Integration Center 437
- National Security Investigations Division 434
- National Security Liaisons 438
- National Security Unit 437
- National Select Agent Registry Program 588
- National Special Security Event (NSSE) 80, 448
- National Strategy for Pandemic Influenza 603
- National Strategy to Secure Cyberspace 226
- National Targeting Center (NTC) 125, 434
- National Targeting Center-Passenger (NTC-P) 434
- National Technical Nuclear Forensics Center 192
- National Terrorism Advisory System (NTAS) 123
- National Threat Assessment Center 82
- National Transportation Security Center of Excellence (NTSCOE) 633
- National Vessel Documentation Center 526
- natural disasters 185, 239, 352
- Naval Postgraduate School 270
- Nazi regime 3
- NBACC *see* National Biodefense Analysis and Countermeasures Center (NBACC)
- NCBSI *see* National Center for Border Security and Immigration (NCBSI)
- NCIRP *see* National Cyber Incident Response Plan (NCIRP)
- NCS *see* National Clandestine Service (NCS)
- NCSC *see* National Counterintelligence and Security Center (NCSC)
- NCSD *see* National Cyber Security Division (NCSD)
- NCTC *see* National Counterterrorism Center (NCTC)
- NDIA *see* National Defense Industrial Association (NDIA)
- NDSP *see* National Dam Safety Program (NDSP)
- Negroponte, John 414
- NEHRP *see* National Earthquake Hazards Reduction Plan (NEHRP)
- NEP *see* National Exercise Program (NEP)
- nerve agents 210
- Network Operations Workstation (NOW) 544
- New Madrid Seismic Zone 258
- New York Police Department (NYPD) 25
- New York State 293
- The New York Times* 28, 600
- NFIP *see* National Flood Insurance Program (NFIP)
- Nielsen, Kirstjen 58
- NROP *see* National Fugitive Operations Program (NFOP)
- NGA *see* National Governors' Association (NGA) Center for Best Practices

- NGIC *see* National Ground Intelligence Center (NGIC)
 NIC *see* National Integration Center (NIC)
 Nicaraguan Adjustment and Central American Relief Act (NACARA) 462
 NII *see* Non-intrusive Inspection (NII) system
 NIMS *see* National Incident Management System (NIMS)
 NIOs *see* National Intelligence officers (NIOs)
 NIPP *see* National Infrastructure Protection Plan (NIPP)
 Nixon, Richard 10, 23
 NLE *see* National Level Exercise (NLE)
 NMIO *see* National Maritime Intelligence-Integration Office (NMIO)
 NNSA *see* National Nuclear Security Administration (NNSA)
 Noble Eagle Operation 522
 nonintrusive inspection (NII) system 512
 Nonprofit Security Grant Program (NSGP) 260
 NORAD *see* North American Aerospace Defense Command (NORAD)
 North American Aerospace Defense Command (NORAD) 47, 334
 North Korea 19
 Northeastern University 632
 NOW *see* Network Operations Workstation (NOW)
 NPD *see* National Preparedness Directorate (NPD)
 NPS *see* National Pharmaceutical Stockpile (NPS)
 NRC *see* Nuclear Regulatory Commission (NRC)
 NRF *see* National Response Framework (NRF)
 NRO *see* National Reconnaissance Office (NRO)
 NSA *see* National Security Agency (NSA)
 NSB *see* National Security Branch (NSB)
 NSGP *see* Nonprofit Security Grant Program (NSGP)
 NSIR *see* Office of Nuclear Security and Incident Response (NSIR)
 NSSE *see* National Special Security Event (NSSE)
 NTAS *see* National Terrorism Advisory System (NTAS)
 NTC *see* National Targeting Center (NTC)
 NTC-P *see* National Targeting Center-Passenger (NTC-P)
 NTSCOE *see* National Transportation Security Center of Excellence (NTSCOE)
 nuclear proliferation 9
 Nuclear Regulatory Commission (NRC) 192
 nuclear weapons 19, 190, 469
 NYPD *see* New York Police Department (NYPD)

 Obama, Barack 53, 94, 103–104, 331, 465
 OBIM *see* Office of Biometric Identity Management (OBIM)
 Occupy Movement 53
 ODNI *see* Office of the Director of National Intelligence (ODNI)
 Office of Biometric Identity Management (OBIM) 66, 112, 475
 Office of Chief Procurement 142
 Office of Civil Rights and Civil Liberties 56
 Office of Community Partnerships 57
 Office of Domestic Nuclear Detection 191
 Office of General Counsel 56
 Office of Grants and Training (G&T) 252
 Office of Ground Water and Drinking Water 566
 Office of Health Affairs 157
 Office of Innovation 140
 Office of Intelligence (OI) 49, 136
 Office of Intelligence and Analysis 290, 309, 395
 Office of Interoperability and Compatibility 132
 Office of Law Enforcement 491
 Office of Legislative Affairs 56
 Office of Management and Budget 118
 Office of Naval Intelligence (ONI) 331
 Office of Nuclear Security and Incident Response (NSIR) 192
 Office of Policy 234
 Office of Port and Facility Compliance 524
 Office of State and Local Government Coordination and Preparedness (SLGCP) 132
 Office of Strategic Trade (OST) 458
 Office of the Director of National Intelligence (ODNI) 396
 Office of the National Counterintelligence Executive (ONCIX) 418
 OI *see* Office of Intelligence (OI)
 Oklahoma City bombing 53, 221, 352, 399
 ONI *see* Office of Naval Intelligence
 open-source Intelligence (OSINT) 404
 Operation Inherent Resolve 331
 Operation Predator program 472
 operations-based exercises 267
 Operations Directorate 136
 Operation Stonegarden (OPSG) 260
 OPSG *see* Operation Stonegarden (OPSG)
 Osama bin Laden 30, 424
 OSINT *see* Open-source Intelligence (OSINT)
 OST *see* Office of Strategic Trade (OST)
 Overstay Analysis Unit 438

 PACER *see* National Center for the Study of Preparedness and Catastrophic Event Response (PACER)
 pandemic flu 592
 pandemic planning 605
 pandemic threats 590–610
 paperless boarding pass 508
 paramount 369
 Partners for Amtrak Safety and Security (PASS) program 544
 Pelfrey, William, Sr., 622
 Pew Research Center 441, 443
 PHMRF *see* Precast Hybrid Movement Resistant Frame (PHMRF) system
 PHOTINT *see* Imagery Intelligence (IMINT)
 photo intelligence (PHOTINT) *see* Imagery Intelligence (IMINT)
 physical fencing 441
 plague 204
 Plum Island Animal Disease Center 578
 Pneumonic Plague 205, 588
 Port and harbor facilities 525
 Port Security Grant Program (PSGP) 260
 Posse Comitatus 106
 Post-Katrina Emergency Reform Act of 2006 252
 Potsdam Convention 6

Index

- PPD-21 *see* Presidential Policy Directive 21 (PPD-21)
Prairie Fire 25
pralidoxime chloride (2-PAM) 218
Precast Hybrid Movement Resistant Frame (PHMRF)
 system 369
predator drone 334
presidential election fraud 228
Presidential Policy Directive 21 (PPD-21) 564
Presidential Proclamation 8607 94
Privacy Office 56
private sector, and homeland security 232–239
Project BioShield Act 587
Project Impact 352
Project Shield America 469
PSGP *see* Port Security Grant Program
PSIC *see* Public Safety Interoperable Communications
 (PSIC)
Public Health Security and Bioterrorism Preparedness
 and Response Act of 2002 565
Public Safety Interoperable Communications (PSIC)
 141, 320
puppy-breeding program 493
Purdue University 632
Putin, Vladimir 13
- radical Islamic fundamentalism 623
radio frequency (RF) 239, 498
radiological, and nuclear terror 47
Radiological Assessment System for Consequence
 Analysis (RASCAL) 195
Radiological dispersal device (RDD) *see* Dirty bomb
Radiological Emergency Preparedness Program 252, 362
rail and mass transit 534–546
rail security coordinator 541
RAMP *see* Risk Assessment and Management Program
 (RAMP)
Rand Commission 325
RASCAL *see* Radiological Assessment System for
 Consequence Analysis (RASCAL)
RCLF *see* Regional, Cultural, and Language
 Familiarization (RCLF) program
Ready.gov 360
Reagan, Ronald 11
REAL ID program 109
Reconstruction Finance Corporation 351
Red Flags 470
Refugee Act of 1980 461
Regional, Cultural, and Language Familiarization
 (RCLF) program 336
regional planning councils 297
Registered Traveler (RT) programs 502
Reno, Janet 28
RF *see* Radio Frequency (RF)
Ricin 210
Ridge, Thomas 52
risk assessment 173–179, 373, 493, 567
Risk Assessment and Management Program
 (RAMP) 176
Robert, John 466
roving wiretaps 107
RSC *see* Rail security coordinator
RT *see* Registered Traveler (RT) program
- Russia
 cold war 6–13
 election interference 104, 228
 generally 15, 109, 227
Rutgers University 632
- S&T *see* Directorate of Science & Technology (S&T)
Saddam Hussein 5, 212, 581
SAFECON program 132, 271
SAFE Port Act 454
SAFER *see* Staffing for Adequate Fire and Emergency
 Response (SAFER)
SAFETY Act *see* Support Antiterrorism by Fostering
 Effective Technologies Act of 2002
San Bernardino shootings 42, 331, 392, 622
sanctuary cities 464, 647–653
Sandy, Hurricane 106, 282, 364
Sandy Hook Elementary School 53, 622
SAR *see* Search and rescue (SAR) team
sarin 208, 212
SBI *see* Secure Border Initiative (SBI)
SBI-net 138
SCADA *see* Supervisory control and data acquisition
 (SCADA)
Schumer, Chuck 159
Schutzstaffel (SS) 3
Science and Technology Directorate 66, 132, 198, 634
Screening of Passengers through Observation
 Techniques (SPOT) program 148
SDS *see* Students for a Democratic Society (SDS)
search and rescue (SAR) team 272, 516
seasonal flu 596
Seattle, dirty bomb in 197
Sector-Specific Agencies (SSA) 539
SECURE™ *see* Systems Efficacy through
 Commercialization, Utilization, Relevance,
 and Evaluation (SECURE™)
Secure Border Initiative (SBI) 136, 438–446
Secure Carton project 513
Secure Flight system 138
Secure Freight Initiative (SFI) 451
Secure Wrap project 513
security, and law enforcement 235, 517, 540
Security and Emergency Management Plan 547
Security and Intelligence Academy 393
security programs, for rail and transit 541–546
security threat assessment (STA) 503
SEPTA *see* Southeastern Pennsylvania Transit Authority
 (SEPTA)
septicemic plague 205
SFI *see* Secure Freight Initiative (SFI)
Shoko Asahara 212
SHSP *see* State Homeland Security Program (SHSP)
Shughart, William, II 357
Signals Intelligence (SIGINT) 338, 390, 404
Sino-Soviet cooperation 10
SLGCP *see* Office of State and Local government
 Coordination and Preparedness (SLGCP)
SLTTGCC *see* State, Local, Tribal, and Territorial
 Government Coordinating Council
 (SLTTGCC)
smallpox 206, 585

- Snowden, Edward 109
 SNS *see* Strategic National Stockpile (SNS)
 soman 211, 218
 South Korea 19
 Southeastern Pennsylvania Transit Authority (SEPTA) 546
 Soviet-style communism 12
 Soviet Union *see* Russia
 SPBIED *see* Suicide pedestrian-borne improvised explosive device (SPBIED)
 Special Security Center 419
 Special Task Force on Detainee Disposition 103
 Speer, Albert 213
 SPOT *see* Screening of Passengers through Observation Techniques (SPOT) program
 SPPA *see* Strategic Partnership Program on Agroterrorism (SPPA)
 SS *see* Schutzstaffel (SS)
 STA *see* Security threat assessment (STA)
 Staffing for Adequate Fire and Emergency Response (SAFER) 259
 Stalin, Joseph 5
 START *see* National Consortium for the Study of Terrorism and Responses to Terrorism (START)
 State, local, tribal, and territorial (SLTT) partners 539
 State, Local, Tribal, and territorial Government Coordinating Council (SLTTGCC) 290
 State Department bombing 24
 state homeland policy 293
 State Homeland Security Program (SHSP) 260
 Stevens Institute of Technology 632
 Strategic National Stockpile (SNS) 121, 588, 603
 Strategic Partnership Program on Agroterrorism (SPPA) 575
 Student and Exchange Visitor Program 438
 Students for a Democratic Society (SDS) 22
 suicide pedestrian-borne improvised explosive device (SPBIED) 221
 suicide vehicle-borne improvised explosive device (SVBIED) 220
 supervisory control and data acquisition (SCADA) 53, 623
 Support Antiterrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) 114
 surveillance
 aerial 126, 158, 334
 electronic 135
 FISA 41
 generally 391, 440, 510, 576, 634
 wiretaps 107
 SVBIED *see* Suicide vehicle-borne improvised explosive device (SVBIED)
 swine flu 592
 Syrian Civil War 208
 Systems Efficacy through Commercialization, Utilization, Relevance, and Evaluation SECURE™, 540
 Tabun 211
 Task Force on State and Local Homeland Security Funding 290
 Tennessee Office of Homeland Security 293
 Terrorist Screening Center (TSC) 404
 Terrorist Threat Integration Center (TTIC) 394
 Texas A&M University 632
 Third Reich 2
 threats and hazards
 biological 198
 concept of 171, 186, 381
 weapons of mass destruction 190
 THSGP *see* Tribal Homeland Security Grant Program (THSGP)
 TOPOFF program 256
 trace portals 497
 Transit Security Grant Program (TSGP) 260
 Transportation Security Administration (TSA)
 canine explosive detection unit 493
 federal air marshals 490
 Federal Flight Deck Officers 491
 generally 482
 law enforcement officers 493
 risk management programs 493
 technology and innovation 497
 Transportation Threat Assessment and Credentialing (TTAC) 139
 Tribal Homeland Security Grant Program (THSGP) 260
 tripwires 407
 Trotskyite-Leninist revolution 6
 Truman, Harry 8
 Trump, Donald J.
 border wall 38, 51, 158–163, 441
 budget appropriations 157, 160
 coronavirus 599
 DHS appointments 51, 57
 election security 227
 executive order 104
 generally 15, 20
 immigration 431, 439, 467
 intelligence gathering 331, 393, 416
 TSA *see* Transportation Security Administration (TSA)
 TSA PreCheck program 148
 TSC *see* Terrorist Screening Center (TSC)
 TSGP *see* Transit Security Grant Program (TSGP)
 TTAC *see* Transportation Threat Assessment and Credentialing (TTAC)
 TTIC *see* Terrorist Threat Integration Center (TTIC)
 twentieth-century military movements 2
 Twin Towers *see* World Trade Center
 UASI *see* Urban Area Security Initiative (UASI)
 UASs *see* Unmanned aircraft systems (UASs)
 UCC *see* Unified Combatant Command (UCC)
 Umar Farouk Abdulmutallab 54
 UNABOM *see* University and Airline Bombing (UNABOM)
 Unabomber *see* Kaczynski, Theodore (Ted)
 Unified Combatant Command (UCC) 106
 United Nations (UN) 19, 104, 206
 United States Computer Emergency Readiness Team (US-CERT) 223
 United States Northern Command (USNORTHCOM) 106
 University and Airline Bombing (UNABOM) 27

Index

- University of Alaska Anchorage 632
- University of Arizona 633
- University of Hawaii 633
- University of Houston 632
- University of Maryland 632
- University of Minnesota 632
- University of Mississippi 357
- University of North Carolina 633
- University of Southern California 632
- University of Texas 633
- Unmanned aircraft systems (UASs) 448
- Urban Area Security Initiative (UASI) 320
- USA Freedom Act of 2015 107
- USAMRIID *see* U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID)
- USA Patriot Act 107, 630
- U.S. Army 123, 337, 401
- U.S. Army Corps of Engineers 351, 369
- U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) 122
- U.S. Border Patrol 461
- US-CERT *see* United States Computer Emergency Readiness Team (US-CERT)
- USCG *see* U.S. Coast Guard (USCG)
- USCIS *see* U.S. Citizenship and Immigration Services (USCIS)
- U.S. Citizenship and Immigration Services (USCIS) 73, 460
- U.S. Coast Guard (USCG) 434, 508, 513–524
- USDA *see* U.S. Department of Agriculture (USDA)
- U.S. Department of Agriculture (USDA) 565, 579
- U.S. Marine Corps (USMC) 335
- USMC *see* U.S. Marine Corps (USMC)
- USNORTHCOM *see* United States Northern Command (USNORTHCOM)
- U.S. Postal Inspection Service 27
- USS Cole 30, 221
- U.S. Secret Service 79, 118, 153
- U.S. Strategic Command (USSTRATCOM) 343
- U.S. Treasury Department 322
- U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) 66, 112, 475
- Variola major *see* smallpox
- vehicle-borne improvised explosive device (VBIED) 567
- vendor managed inventory (VMI) 121
- vessel inspection 526
- VGT *see* Virtual Global Taskforce (VGT)
- Vietnam War 10
- VIPR *see* Visible Intermodal Prevention and Response (VIPR)
- Virtual Global Taskforce (VGT) 472
- visa issuance 57, 404, 436; *see also* Diversity Immigrant Visa Program (DV Program)
- Visible Intermodal Prevention and Response (VIPR) 486
- VMI *see* Vendor managed inventory (VMI)
- vulnerability assessment 226, 509, 563
- VX 211
- Wannsee Conference 3
- The Washington Post* 28
- water 565–571
- waterways 510, 522
- Water Security Division (WSD) 566
- Wagh, William L., Jr., 629
- weapons of mass destruction (WMD)
 - biological 198–206
 - chemical 206–219
 - improvised explosive devices 218–222
 - nuclear 190–198
 - radiological 196–198
- Weathermen 22–24
- WHO *see* World Health Organization (WHO)
- WIRe *see* World Intelligence Review (WIRe)
- WMD *see* Weapons of mass destruction (WMD)
- Wolf, Chad 59
- World Health Organization (WHO) 590–599
- World Intelligence Review (WIRe) 410
- World Trade Center 25, 36, 399
- World War I (WWI) 2, 208, 581
- World War II (WWII) 2, 212, 399
- WSD *see* Water Security Division (WSD)
- Wuhan, China 595, 599
- WWI *see* World War I (WWI)
- WWII *see* World War II (WWII)
- Yersinia pestis* *see* plague
- zero-tolerance policy 58
- Zoonotic and Animal Disease Defense (ZADD) 632